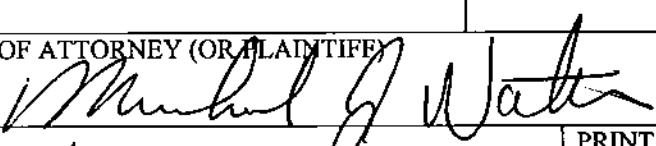


ADVERSARY PROCEEDING COVER SHEET (Instructions on Reverse)		ADVERSARY PROCEEDING NUMBER (Court use only)
<b>PLAINTIFFS</b> Rene R. Ortiz 1512 Cleveland Avenue Racine, WI 53405  Douglas Lynn Lindsey 18 East Sedgemoor Street Elkhorn, WI 53121  Valerie Jones 7754 North Mariners Street Milwaukee, WI 53224	<b>DEFENDANT</b> Aurora Health Care, Inc. c/o Nick Turkal 3000 West Montana Avenue Milwaukee, WI 53215	
ATTORNEYS (Firm Name, Address, and Telephone No.) Michael J. Watton Watton Law Group 225 East Michigan Street, Suite 550 Milwaukee, WI 53202 (414) 273-6858	ATTORNEYS (If Known)	
<b>PARTY</b> (Check One Box Only) <input checked="" type="checkbox"/> Debtor <input type="checkbox"/> U.S. Trustee/Bankruptcy Admin <input type="checkbox"/> Creditor <input type="checkbox"/> Other <input type="checkbox"/> Trustee	<b>PARTY</b> (Check One Box Only) <input type="checkbox"/> Debtor <input type="checkbox"/> U.S. Trustee/Bankruptcy Admin <input checked="" type="checkbox"/> Creditor <input type="checkbox"/> Other <input type="checkbox"/> Trustee	
<b>CAUSE OF ACTION</b> (WRITE A BRIEF STATEMENT OF CAUSE OF ACTION, INCLUDING ALL U.S. STATUTES INVOLVED) Violation of the Wis. Stat. § 146.82 and Contempt of Court for Violation of FRBP 9037		
<b>NATURE OF SUIT</b> (Number up to five (5) boxes starting with lead cause of action as 1, first alternative cause as 2, second alternative as 3 etc.)		
<b>FRBP 7001(1) – Recovery of money/property</b> <input type="checkbox"/> 11- Recovery of money/property - §542 turnover of property <input type="checkbox"/> 12- Recovery of money/property - §547 preference <input type="checkbox"/> 13- Recovery of money/property - §548 fraudulent transfer <input checked="" type="checkbox"/> 14- Recovery of money/property - other <b>FRBP 7001(2) – Validity, Priority or Extent of Lien</b> <input type="checkbox"/> 21- Validity, priority or extent of lien or other interest in property <b>FRBP 7001(3) – Approval of Sale of Property</b> <input type="checkbox"/> 31- Approval of sale of property of estate and of a co-owner - §363(h) <b>FRBP 7001(4) – Objection/Revocation of Discharge</b> <input type="checkbox"/> 41- Objection / revocation of discharge - §727(c),(d),(e) <b>FRBP 7001(5) – Revocation of Confirmation</b> <input type="checkbox"/> 51- Revocation of confirmation <b>FRBP 7001(6) - Dischargeability</b> <input type="checkbox"/> 66- Dischargeability - §523(a)(1),(14),(14A) priority tax claims <input type="checkbox"/> 62- Dischargeability - §523(a)(2), false pretenses, false representation, actual fraud <input type="checkbox"/> 67- Dischargeability - §523(a)(4), fraud as fiduciary, embezzlement, larceny  (Continued on next column)	<b>FRBP 7001(6) – Dischargeability (continued)</b> <input type="checkbox"/> 61- Dischargeability - §523(a)(5), domestic support <input type="checkbox"/> 68- Dischargeability - §523(a)(6), willful and malicious injury <input type="checkbox"/> 63- Dischargeability - §523(a)(8), student loan <input type="checkbox"/> 64- Dischargeability - §523(a)(15), divorce or separation obligation (other than domestic support) <input type="checkbox"/> 65- Dischargeability - other <b>FRBP 7001(7) – Injunction Relief</b> <input type="checkbox"/> 71- Injunctive relief – reinstatement of stay <input checked="" type="checkbox"/> 72- Injunctive relief – other <b>FRBP 7001(8) – Subordination of Claim or Interest</b> <input type="checkbox"/> 81- Subordination of claim or interest <b>FRBP 7001(9) Declaratory Judgment</b> <input type="checkbox"/> 91- Declaratory judgment <b>FRBP 7001(10) Determination of Removed Action</b> <input type="checkbox"/> 01- Determination of removed claim or cause <b>Other</b> <input type="checkbox"/> SS-SIPA Case -15 U.S.C. §§78aaa <i>et seq.</i> <input checked="" type="checkbox"/> 02-Other (e.g. other actions that would have been brought in state court if unrelated to bankruptcy case)	
<input checked="" type="checkbox"/> Check if this case involves a substantive issue of state law	<input checked="" type="checkbox"/> Check if this is asserted to be a class action under FRCP 23	
<input checked="" type="checkbox"/> Check if a jury trial is demanded in complaint	Demand \$ To be determined	
Other Relief Sought: Order Defendant in civil contempt for violating the established policies, rules and orders of the Court, and damages for Defendant's actions. Further order damages for Defendant's violation of Wis. Stat. § 146.82.		

**BANKRUPTCY CASE IN WHICH THIS ADVERSARY PROCEEDING ARISES**

NAME OF DEBTOR: Rene Ortiz; Douglas Lynn Lindsey; Valerie Jones; all others similarly situated		BANKRUPTCY CASE NO.: 07-22466-SVK; 08-27374-SVK; 07-25336-SVK	
DISTRICT WHICH CASE IS PENDING Eastern District of Wisconsin	DIVISIONAL OFFICE	NAME OF JUDGE Susan V. Kelley	
<b>RELATED ADVERSARY PROCEEDING (IF ANY)</b>			
PLAINTIFF	DEFENDANT	ADVERSARY PROCEEDING NO.	
DISTRICT IN WHICH ADVERSARY IS PENDING	DIVISIONAL OFFICE	NAME OF JUDGE	
SIGNATURE OF ATTORNEY (OR PLAINTIFF) 			
DATE 6-23-09	PRINT NAME OF ATTORNEY (OR PLAINTIFF) Michael J. Watton, Esq.		

**INSTRUCTIONS**

The filing of a bankruptcy case creates an "estate" under the jurisdiction of the bankruptcy court which consists of all of the property of the debtor, wherever that property is located. Because the bankruptcy estate is so extensive and the jurisdiction of the court so broad, there may be lawsuits over the property or property rights of the estate. There also may be lawsuits concerning the debtor's discharge. If such a lawsuit is filed in a bankruptcy court, it is called an adversary proceeding.

A party filing an adversary proceeding must also complete and file Form 104, the Adversary Proceeding Cover Sheet, if it is required by the court. In some courts, the cover sheet is not required when the adversary proceeding is filed electronically through the court's Case Management/Electronic Case Files (CM/ECF) system. (CM/ECF captures the information on Form 104 as part of the filing process.) When completed, the cover sheet summarizes basic information on the adversary proceeding. The clerk of court needs the information to process the adversary proceeding and prepare required statistical reports on court activity.

The cover sheet and the information contained on it do not replace or supplement the filing and service of pleadings or other papers as required by law, the Bankruptcy Rules, or the local rules of court. The cover sheet, which is largely self-explanatory, must be completed by the plaintiff's attorney (or by the plaintiff if the plaintiff is not represented by an attorney). A separate cover sheet must be submitted to the clerk for each complaint filed.

**Plaintiffs and Defendants.** Give the names of the plaintiffs and the defendants exactly as they appear on the complaint.

**Attorneys.** Give the names and addresses of the attorneys, if known.

**Party.** Check the most appropriate box in the first column for the plaintiffs and in the second column for the defendants.

**Demand.** Enter the dollar amount being demanded in the complaint.

**Signature.** This cover sheet must be signed by the attorney of record in the box on the second page of the form. If the plaintiff is represented by a law firm, a member of the firm must sign. If the plaintiff is pro se, that is, not represented by an attorney, the plaintiff must sign.

**UNITED STATES BANKRUPTCY COURT  
EASTERN DISTRICT OF WISCONSIN**

In re Rene R. Ortiz,	)	
In re Douglas Lynn Lindsey and	)	
Betty Jane Lindsey,	)	
In re Valerie Jones,	)	
	)	ALL DOCUMENTS REGARDING THIS MATTER MUST BE
Debtors.	)	IDENTIFIED BY BOTH ADVERSARY AND BANKRUPTCY
	)	CASE NUMBERS.
Rene R. Ortiz, Douglas Lynn Lindsey,	)	
Valerie Jones, on behalf of themselves,	)	
their individual bankruptcy estates and all	)	Bankruptcy Case No. 07-22466-SVK
others similarly situated,	)	Bankruptcy Case No. 08-27374-SVK
	)	Bankruptcy Case No. 07-25336-SVK
Plaintiffs,	)	
v.	)	Adversary Proceeding No.
Aurora Health Care, Inc.	)	
	)	
Defendant.	)	

**SUMMONS AND NOTICE OF PRETRIAL CONFERENCE  
IN AN ADVERSARY PROCEEDING**

YOU ARE SUMMONED and required to submit a motion or answer to the complaint which is attached to this summons to the clerk of the bankruptcy court within 30 days after the date of issuance of this summons, except that the United States and its offices and agencies shall submit a motion or answer to the complaint within 35 days.

Address of Clerk	Clerk, U.S. Bankruptcy Court U.S. Courthouse, Room 126 517 East Wisconsin Avenue Milwaukee, WI 53202
------------------	---

At the same time, you must also serve a copy of the motion or answer upon the plaintiff's attorney.

Name and Address of Plaintiff's Attorney

Michael J. Watton, Esq. Watton Law Group 225 East Michigan Street, Suite 550 Milwaukee, WI 53202
---

If you make a motion, your time to answer is governed by Fed. R. Bankr. P. 7012.

YOU ARE NOTIFIED that a pretrial conference of the proceeding commenced by the filing of the complaint will be held at the following time and place.

Address

Room, Date and Time

**IF YOU FAIL TO RESPOND TO THIS SUMMONS, YOUR FAILURE WILL BE DEEMED TO BE YOUR CONSENT TO ENTRY OF A JUDGEMENT BY THE BANKRUPTCY COURT AND JUDGEMENT BY DEFAULT MAY BE TAKEN AGAINST YOU FOR THE RELIEF DEMANDED IN THE COMPLAINT. IF A PARTY FAILS TO APPEAR, JUDGEMENT OR DISMISSAL MAY BE GRANTED WITHOUT FURTHER HEARING.**

Christopher L. Austin  
*Clerk of the Bankruptcy Court*

By:

Date

Case 09-02199-svk Doc 1 Filed 06/23/09

Deputy Clerk

Page 3 of 46

UNITED STATES BANKRUPTCY COURT  
EASTERN DISTRICT OF WISCONSIN

In re Rene R. Ortiz,	)	Bankruptcy Case No. 07-22466-SVK
In re Douglas Lynn Lindsey and	)	
Betty Jane Lindsey,	)	Bankruptcy Case No. 08-27374-SVK
In re Valerie Jones,	)	Bankruptcy Case No. 07-25336-SVK
Debtors.	)	
Rene R. Ortiz, Douglas Lynn Lindsey,	)	
Valerie Jones, on behalf of themselves,	)	
their individual bankruptcy estates and all	)	
others similarly situated,	)	Case No.
Plaintiffs,	)	
v.	)	
Aurora Health Care, Inc.	)	
Defendant.	)	

---

Plaintiffs Rene R. Ortiz, Douglas Lynn Lindsey, and Valerie Jones, on behalf of themselves, their individual bankruptcy estates and all others similarly situated, by and through their attorneys, allege to the best of their knowledge, information and belief, formed after inquiry reasonable under the circumstances, as follows:

**INTRODUCTION**

1. This lawsuit seeks class-wide relief for persons who have filed for Chapter 13 bankruptcy in the Eastern District of Wisconsin and have proofs of claim filed in the public

Michael J. Watton, Esq.  
Watton Law Group  
225 East Michigan Street  
Suite 550  
Milwaukee, WI 53202  
414-273-6858

record against their estates by Defendant Aurora Health Care, Inc. Proofs of Claim filed by Defendant disclose private medical treatment and records as attachments to each proof. Defendant Aurora Health Care, Inc.'s policy has been to file along with any proof of claim attachments which violate state and federal privacy statutes.

2. Defendant's public revelations of the Plaintiffs' individual private, sensitive, confidential health care records, knowingly exposes all Plaintiffs to emotional embarrassment, medical identity theft and identity theft.

3. Causes of Action herein are brought against Defendant under the United States Bankruptcy Code ("Bankruptcy Code"), 11 U.S.C. §101, *et. seq.*, for violation of Wis. Stat. §146.82 for Breach of Confidentiality of Patient Health Care Records and for mandatory injunctive relief requiring the Defendant to Motion the Court in each case to restrict the viewing of the claims Defendant filed to date and requiring Defendant to file substitute redacted claims to comply with Federal Rule of Bankruptcy Procedure 9037 for Failure to Redact Nonpublic information.

#### **JURISDICTION AND VENUE**

4. This Court has jurisdiction over these proceedings via 28 U.S.C. §§ 1334 and 1367. This is a "core proceeding" under the Bankruptcy Code because it concerns substantive bankruptcy issues that could only arise in the bankruptcy context and concern the administration of the estate. 28 U.S.C. §157(b)(2)(A), (C), and (O).

5. Venue is appropriate under 28 U.S.C. §1409 in that the Plaintiffs all filed for Chapter 13 bankruptcy protection in this jurisdiction and Defendant routinely avails itself of the bankruptcy courts in this jurisdiction to assert claims as a creditor.

6. This is an adversary proceeding to recover money or property pursuant to Bankruptcy Rule 7001(1) and for injunctive relief pursuant to Rule 7001(7).

## **PARTIES**

**7.** Plaintiff Rene R. Ortiz filed for Chapter 13 bankruptcy protection in this judicial district on April 6, 2007 and his case was assigned the number 07-22466 (the “Ortiz Bankruptcy”).

**8.** Plaintiffs Douglas and Betty Lindsey filed for Chapter 13 bankruptcy protection in this judicial district with his wife Betty Lindsey (now deceased) on July 8, 2008 and their case was assigned number 08-27374 (the “Lindsey Bankruptcy”).

**9.** Plaintiff Valerie Jones filed for Chapter 13 bankruptcy protection in this judicial district on July 12, 2007 and her case was assigned the number 07-25336 (the “Jones Bankruptcy”).

**10.** Defendant Aurora Health Care, Inc. is a Wisconsin corporation with a principal office at 3000 West Montana Avenue, Milwaukee, WI 53215. Defendant’s registered agent is Nick Turkal at the same address.

## **COMMON FACTS RELATED TO ALL BANKRUPTCY CASES**

**11.** Upon information and belief, Defendant maintains a department of professionals to insure Defendant’s compliance with governmental regulation over healthcare providers.

**12.** Defendant is well aware of HIPAA regulations requiring privacy of medical information.

**13.** Defendant also maintains professionals on staff to collect funds from patients for medical services.

**14.** The Federal Government’s Privacy Rule regulating conduct disclosing medical information is enumerated in the Federal Register at 65 Fed. Reg. at 82464. (Exhibit A) This clear rule became effective on April 14, 2003, and established regulations and standards for the

use and disclosure of Protected Health Information. Protected Health Information is any information about health status, provision of health care, or payment for health care that can be linked to an individual. This is interpreted rather broadly and includes any part of a patient's medical record or payment history.

**15.** The Privacy Rule is a Health & Human Services regulation pursuant to numerous federal laws, including but not limited to, the Health Insurance Portability and Accountability Act of 1996 (HIPPA). See, 65 Fed. Reg. at 82469. (Exhibit A).

**16.** According to the rule, a covered entity may disclose protected health information to facilitate treatment, payment, or health care operations or if the covered entity has obtained authorization from the individual. However, when a covered entity discloses any protected health information it must make a reasonable effort to disclose only the minimum necessary information required to achieve its purpose. (Exhibit A)

**17.** On September 29, 2003 and December 1, 2007, the United States District Court for the Eastern District of Wisconsin issued Procedural Orders governing the protection of personal and sensitive information and public access to court files in accordance with the E-Government Act of 2002. (Exhibits B and C)

**18.** The Orders cautioned that un-redacted disclosures of personal identifiers were prohibited.

**19.** The Orders specify the Court's policy that certain personal data identifiers must be partially redacted from the case filing or pleading. Specifically listed as examples of "personal data identifiers" are (1) social security numbers, (2) financial account numbers, (3) birth dates, (4) medical records, treatment and diagnosis. (Exhibits B and C)

**20.** The United States Bankruptcy Court of the Eastern District of Wisconsin as an

adjunct court of the United States District Court for the Eastern District of Wisconsin, has adopted the Rules, and is subject to the Orders of the United States District Court for the Eastern District of Wisconsin.

21. On or about September 2, 2008, the United States Bankruptcy Court of the Eastern District of Wisconsin issued a Privacy Reminder both on the Court's web-site (<http://www.wieb.uscourts.gov/index.php>) and on the initial log-in page to the Court's (<http://ecf.wieb.uscourts.gov/cgi-bin/login.pl>) CM/ECF electronic filing site which states:

**Privacy Rule Reminder:** To protect the rights of debtors and creditors, Bankruptcy Rule 9037 requires that certain personal data identifiers be modified or redacted from Bankruptcy Court case files. While there are limited exceptions, only the following should appear in filings made with the Bankruptcy Court:

- only the last four digits of an individual's social security number or taxpayer identification number
- only the last four digits of a financial account number
- only the year of an individual's birth
- only the initials of a minor.

**Please note it is the responsibility of the attorney or party making the filing with the court to redact the personal information.** The clerk will not review documents and remove personal information. Special rules apply for transcripts that are filed with the Court. See the Transcripts tab of this website for more information. Consult Bankruptcy Rule 9037 for exemptions from the redaction requirements. If you or another party in a case has filed personal identifiers, you may file a Motion to Restrict Viewing of that document to court staff only. Please contact us with questions about the Privacy Rule.

22. On December 1, 2007, the Federal Rule of Bankruptcy Procedure 9037 and Federal Rule of Civil Procedure 5.2 went into effect further strengthening and reinforcing the Court's local rules and policies. (Exhibit D and E)

23. Rule 9037 is titled Privacy Protection for Filings Made with the Court and provides that:

- (a) REDACTED FILINGS. Unless the court orders otherwise, in an electronic or paper filing with the court that contains an individual's social security number, taxpayer identification number, or birth date, the name of an

individual, other than the debtor, known to be and identified as a minor, or a financial account number, a party or nonparty making the filing may include only:

- (1) the last four digits of the social security number and taxpayer identification number;
- (2) the year of the individual's birth;
- (3) the minor's initials; and
- (4) the last four digits of the financial account number.

**24.** Defendant is a sophisticated medical provider and a covered entity with knowledge of the rules and regulations governing protection and privacy of Individually Identifiable Health Information and knowledge of the bankruptcy rules and procedures. Defendant has an obligation to comply with all applicable rules and statutes when filing claims and participating in the bankruptcy process.

**25.** Defendant has previously been the subject of a lawsuit, Ottow v. Aurora Health Care, EDWI, Adv. Proc. No. 08-02274.

**26.** On information and belief Aurora settled the lawsuit privately, its representatives understood that redaction was required and has willfully ignored the harm it has created to others besides the Ottow plaintiffs. See Exhibit F.

**27.** Defendant has intentionally communicated or otherwise made available to the general public the personal, sensitive and private data and protected health information.

**28.** The proofs of claim filed by Defendant with medical procedures and treatment information remain in the public record as of the date of the filing of this complaint.

#### **FACTS GIVING RISE TO THE CAUSES OF ACTION – ORTIZ BANKRUPTCY**

**29.** Mr. Ortiz incurred a debt to Defendant sometime prior to the filing of his Chapter 13 bankruptcy. The debt was for primarily consumer healthcare.

**30.** On two occasions Defendant filed proofs of claim revealing Rene R. Ortiz's confidential medical information.

31. Proofs of claim number 8 and 9 in the Ortiz Bankruptcy publicly reveals medical procedures and treatment. Claim number 8 is dated 5/29/07 and is signed by Barb Brooks, Supervisor/Hospital Collections. Claim number 9 is dated July 19, 2007 and is signed by Stephanie Herron, Supervisor of Collections.

32. Each proof of claim contained a number of pages and displayed Mr. Ortiz's account and invoice numbers, address and other sensitive data including the unauthorized disclosure of Mr. Ortiz's individually identifiable health information, with treatment and medical equipment usage, without redaction.

33. The proofs of claim are public documents and Defendant has made and continues to make Mr. Ortiz's private, sensitive, nonpublic, personal medical information available to the general public.

#### **FACTS GIVING RISE TO THE CAUSES OF ACTION – LINDSEY BANKRUPTCY**

34. Mr. and Mrs. Lindsey incurred a debt to Defendant sometime prior to the filing of their Chapter 13 bankruptcy. The debt was for primarily consumer healthcare.

35. On two occasions Defendant filed proofs of claim revealing Doug and Betty Lindsey's confidential medical information.

36. Proofs of claim 4 and 8 in the Lindsey Bankruptcy publicly reveals medical procedures and treatment. Claim number 4 is dated July 30, 2008 and is signed by Tammy Fiedler, Collection Specialist. Claim number 8 is dated August 26, 2008 and is signed by Barb Brooks, Supervisor/Hospital Collections.

37. Each Proof of Claim contained a number of pages and displayed Mr. and Mrs.

Lindsey's account and invoice numbers, address and other sensitive data including the unauthorized disclosure of Mr. and Mrs. Lindsey's individually identifiable health information, with treatment and medical equipment usage, without redaction.

**38.** The Proofs of claim are public documents and Defendant has made and continues to make Mr. and Mrs. Lindsey's private, sensitive, nonpublic, personal medical information available to the general public.

#### **FACTS GIVING RISE TO THE CAUSES OF ACTION – JONES BANKRUPTCY**

**39.** Ms. Jones incurred a debt to Defendant sometime prior to the filing of her Chapter 13 bankruptcy. The debt was for primarily consumer healthcare.

**40.** On one occasion Defendant filed a proof of claim revealing Valerie Jones' confidential medical information.

**41.** Proof of claim 5 in the Jones bankruptcy publicly reveals medical procedures and treatment. Claim 5 is dated August 9, 2007 and is signed by Tammy Fiedler, Collection Specialist.

**42.** The Proof of claim contains a number of pages and displays Ms. Jones' account and invoice numbers, address and other sensitive data including the unauthorized disclosure of Ms. Jones' individually identifiable health information, with treatment and medical equipment usage, without redaction.

**43.** The Proof of claim is a public document and Defendant has made and continues to make Ms. Jones' private, sensitive, nonpublic, personal medical information available to the general public.

#### **CLASS ALLEGATIONS**

**44.** Plaintiffs bring this class action pursuant to Federal Rule of Bankruptcy Procedure 7023 which makes Federal Rule of Civil Procedure 23 applicable in the bankruptcy courts.

Specifically, Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure are asserted on behalf of a class consisting of all persons who filed a petition for relief under Chapter 13 of the Bankruptcy Code, (and their estates) in circumstances in which Aurora Health Care filed at least one proof of claim which includes sensitive, personal and confidential information about medical treatment and usage.

45. The members of the class are so numerous that joinder of all members is impracticable.

46. Plaintiffs' claims are typical of the claims of the class and plaintiffs and the class sustain ongoing damages from Aurora Health Care's wrongful conduct.

47. Plaintiffs will adequately protect the interests of the class. Plaintiffs have retained lawyers who are experienced and competent in class action litigation. Plaintiffs have no interests that conflict with those of the class.

48. Aurora Health Care has acted in a manner and on grounds generally applicable to the class, thereby making appropriate final mandatory injunctive and declaratory relief with respect to the class as a whole.

49. Common questions of law and fact predominate over questions that affect only individual members. Among the questions of law and fact common to the class are:

- (a) Whether Aurora is permitted publicly reveal plaintiffs' confidential medical information in the public record?
- (b) Whether the bankruptcy court has the power to require Aurora to comply with its rules?
- (c) Whether Aurora's actions and lack of corrective action was knowing and willful given its employees knowledge of privacy laws and at least one prior lawsuit ?
- (d) Whether Aurora is required to move the Court for a Motion To Restrict Viewing

in each individual bankruptcy case it revealed confidential information?

(e) Whether Aurora is required to file substitute proofs of claims in each case to maintain their individual bankruptcy claims?

(f) Whether the acts of Aurora applies to the class as a whole, entitling the class to mandatory injunctive relief as well as damages?

50. A class action is superior to other available methods for the fair and efficient adjudication of this controversy.

**FIRST CAUSE OF ACTION:  
MANDATORY PERMANENT INJUNCTIVE RELIEF- Class Action**

51. Plaintiffs specifically reallege each of the foregoing paragraphs as though fully set out herein.

52. This Court entitled to issue injunctive relief when necessary. See, Fed.R. Bankr. Proc. 7001 (7).

53. The Court may issue orders that are necessary to carry out title 11. 11 U.S.C. §105(a).

54. Defendant continues to harm it debtors who avail themselves of the Chapter 13 protective mechanism by making public and leaving in the public record unredacted, sensitive, personal and confidential medical information.

55. The affect of Defendant's actions is to dissuade future debtors in need of court protection to risk disclosure of sensitive, private and confidential information to the public.

56. Defendant is well aware of HIPAA and its purpose.

57. Defendant has knowledge of Bankruptcy Rule 9037 and District Court Orders dated September 29, 2003 and December 1, 2007.

58. Defendant has knowledge of its own settlement and the court orders in Ottow v.

Aurora Health Care, EDWI, Adv. Proc. No. 08-02274.

**59.** The District Court Orders entered September 29, 2003, December 1, 2007 and Bankruptcy Rule 9037 prohibit the filing of "personal information."

**60.** All proofs of claim filed by Defendant Aurora in the Ortiz Bankruptcy, the Lindsey Bankruptcy and the Jones Bankruptcy include medical records, treatment, and diagnosis.

**61.** By failing to redact or delete the personal information in all 5 instances referenced above, Defendant willfully violated the Bankruptcy Rules and District Court orders.

**62.** Defendant has handled all class members proofs of claim in a like manner to those in the Ortiz Bankruptcy, the Lindsey Bankruptcy and the Jones Bankruptcy.

**63.** A mandatory injunction must issue to compel Defendant to expend the resources necessary to Motion the Court in each underlying case for an order sealing from the public record the proofs of claim it has filed in all cases both for the named plaintiffs and the putative class.

**SECOND CAUSE OF ACTION:  
VIOLATION OF WIS. STAT. § 146.82 FOR BREACH OF  
CONFIDENTIALITY OF PATIENT HEALTH CARE RECORDS- Class Action**

**64.** Plaintiffs specifically reallege each of the foregoing paragraphs as though fully set out herein.

**65.** Defendant is a "health care provider" within the meaning of Wis. Stat. § 146.81.

**66.** Defendant maintained the "patient health care records" of Mr. Ortiz, Mr. and Mrs. Lindsey and Ms. Jones within the meaning of Wis. Stat. § 146.81.

**67.** Defendant had a duty pursuant to Wis. Stat. § 146.82 to keep all "patient health care records" of all Plaintiffs and all putative class plaintiffs confidential.

**68.** Defendant has willfully, intentionally and recklessly disclosed nonpublic, personal

information by releasing portions of Plaintiffs' and all putative class plaintiffs patient health care records in a public records forum.

69. As a result of Defendant's willful, indifferent and direct violation of Wis. Stat. § 148.82, named Plaintiffs and putative class plaintiffs have suffered actual damages and injury, exemplary damages, and attorneys' fees and costs within the meaning of Wis. Stat. § 146.84.

**WHEREFORE**, Plaintiffs pray for the following relief:

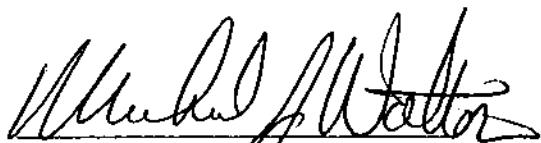
- A. a declaratory finding that Defendant has violated the established policies, rules and orders of the Court in establishing privacy standards.
- B. a mandatory injunction requiring Defendant file Motions for Restricted Access to all claims in each and every underlying case for all named and putative class plaintiffs and file substitute claims.
- C. a monetary award of exemplary damages of \$25,000 per class member, actual damages, costs and reasonable attorneys' fees against Defendant for each person whose private and sensitive data including, confidential health care records have been publicly revealed in the Bankruptcy Court's Public Access to Court Electronic Records (PACER). Damages should include knowingly exposing named and putative class plaintiffs to the risk of medical identity theft and identity theft. Wis. Stat. §146.84.
- D. a monetary award of exemplary damages and attorneys' fees and costs as specified in Wis. Stat. § 146.84.

...

...

E. for such other and further relief as the Court may deem just and proper.

Dated this 23<sup>rd</sup> day of June, 2009



Michael J. Watton, Esq.

Michael J. Maloney, Esq.

Victoria Kies Garoukian, Esq.

Watton Law Group

225 E. Michigan Street, Suite 550

Milwaukee, Wisconsin 53202

however, found that "state laws, with a few notable exceptions, do not extend comprehensive protections to people's medical records." Many state rules fail to provide such basic protections as ensuring a patient's legal right to see a copy of his or her medical record. See Health Privacy Project, "The State of Health Privacy: An Uneven Terrain," Institute for Health Care Research and Policy, Georgetown University (July 1999) (<http://www.healthprivacy.org>) (the "Georgetown Study").

Until now, virtually no federal rules existed to protect the privacy of health information and guarantee patient access to such information. This final rule establishes, for the first time, a set of basic national privacy standards and fair information practices that provides all Americans with a basic level of protection and peace of mind that is essential to their full participation in their care. The rule sets a floor of ground rules for health care providers, health plans, and health care clearinghouses to follow, in order to protect patients and encourage them to seek needed care. The rule seeks to balance the needs of the individual with the needs of the society. It creates a framework of protection that can be strengthened by both the federal government and by states as health information systems continue to evolve.

#### *Need for a National Health Privacy Framework*

#### *The Importance of Privacy*

Privacy is a fundamental right. As such, it must be viewed differently than any ordinary economic good. The costs and benefits of a regulation must, of course, be considered as a means of identifying and weighing options. At the same time, it is important not to lose sight of the inherent meaning of privacy: it speaks to our individual and collective freedom.

A right to privacy in personal information has historically found expression in American law. All fifty states today recognize in tort law a common law or statutory right to privacy. Many states specifically provide a remedy for public revelation of private facts. Some states, such as California and Tennessee, have a right to privacy as a matter of state constitutional law. The multiple historical sources for legal rights to privacy are traced in many places, including Chapter 13 of Alan Westin's *Privacy and Freedom* and in Ellen Alderman & Caroline Kennedy, *The Right to Privacy* (1995).

Throughout our nation's history, we have placed the rights of the individual

at the forefront of our democracy. In the Declaration of Independence, we asserted the "unalienable right" to "life, liberty and the pursuit of happiness." Many of the most basic protections in the Constitution of the United States are imbued with an attempt to protect individual privacy while balancing it against the larger social purposes of the nation.

To take but one example, the Fourth Amendment to the United States Constitution guarantees that "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated." By referring to the need for security of "persons" as well as "papers and effects" the Fourth Amendment suggests enduring values in American law that relate to privacy. The need for security of "persons" is consistent with obtaining patient consent before performing invasive medical procedures. The need for security in "papers and effects" underscores the importance of protecting information about the person, contained in sources such as personal diaries, medical records, or elsewhere. As is generally true for the right of privacy in information, the right is not absolute. The test instead is what constitutes an "unreasonable" search of the papers and effects.

The United States Supreme Court has upheld the constitutional protection of personal health information. In *Whalen v. Roe*, 429 U.S. 589 (1977), the Court analyzed a New York statute that created a database of persons who obtained drugs for which there was both a lawful and unlawful market. The Court, in upholding the statute, recognized at least two different kinds of interests within the constitutionally protected "zone of privacy." "One is the individual interest in avoiding disclosure of personal matters," such as this regulation principally addresses. This interest in avoiding disclosure, discussed in Whalen in the context of medical information, was found to be distinct from a different line of cases concerning "the interest in independence in making certain kinds of important decisions."

Individuals' right to privacy in information about themselves is not absolute. It does not, for instance, prevent reporting of public health information on communicable diseases or stop law enforcement from getting information when due process has been observed. But many people believe that individuals should have some right to control personal and sensitive information about themselves. Among

different sorts of personal information, health information is among the most sensitive. Many people believe that details about their physical self should not generally be put on display for neighbors, employers, and government officials to see. Informed consent laws place limits on the ability of other persons to intrude physically on a person's body. Similar concerns apply to intrusions on information about the person.

Moving beyond these facts of physical treatment, there is also significant intrusion when records reveal details about a person's mental state, such as during treatment for mental health. If, in Justice Brandeis' words, the "right to be let alone" means anything, then it likely applies to having outsiders have access to one's intimate thoughts, words, and emotions. In the recent case of *Jaffee v. Redmond*, 116 S.Ct. 1923 (1996), the Supreme Court held that statements made to a therapist during a counseling session were protected against civil discovery under the Federal Rules of Evidence. The Court noted that all fifty states have adopted some form of the psychotherapist-patient privilege. In upholding the federal privilege, the Supreme Court stated that it "serves the public interest by facilitating the appropriate treatment for individuals suffering the effects of a mental or emotional problem. The mental health of our citizenry, no less than its physical health, is a public good of transcendent importance."

Many writers have urged a philosophical or common-sense right to privacy in one's personal information. Examples include Alan Westin, *Privacy and Freedom* (1967) and Janna Malamud Smith, *Private Matters: In Defense of the Personal Life* (1997). These writings emphasize the link between privacy and freedom and privacy and the "personal life," or the ability to develop one's own personality and self-expression. Smith, for instance, states:

The bottom line is clear. If we continually, gratuitously, reveal other people's privacies, we harm them and ourselves, we undermine the richness of the personal life, and we fuel a social atmosphere of mutual exploitation. Let me put it another way: Little in life is as precious as the freedom to say and do things with people you love that you would not say or do if someone else were present. And few experiences are as fundamental to liberty and autonomy as maintaining control over when, how, to whom, and where you disclose personal material. *Id.* at 240-241.

In 1890, Louis D. Brandeis and Samuel D. Warren defined the right to privacy as "the right to be let alone." See L. Brandeis, S. Warren, "The Right

To Privacy," 4 Harv.L.Rev. 193. More than a century later, privacy continues to play an important role in Americans' lives. In their book, *The Right to Privacy*, (Alfred A. Knopf, New York, 1995) Ellen Alderman and Caroline Kennedy describe the importance of privacy in this way:

Privacy covers many things. It protects the solitude necessary for creative thought. It allows us the independence that is part of raising a family. It protects our right to be secure in our own homes and possessions, assured that the government cannot come barging in. Privacy also encompasses our right to self-determination and to define who we are. Although we live in a world of noisy self-confession, privacy allows us to keep certain facts to ourselves if we so choose. The right to privacy, it seems, is what makes us civilized.

Or, as Cavoukian and Tapscott observed the right of privacy is: "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated." See A. Cavoukian, D. Tapscott, "Who Knows: Safeguarding Your Privacy in a Networked World," Random House (1995).

#### *Increasing Public Concern About Loss of Privacy*

Today, it is virtually impossible for any person to be truly "let alone." The average American is inundated with requests for information from potential employers, retail shops, telephone marketing firms, electronic marketers, banks, insurance companies, hospitals, physicians, health plans, and others. In a 1998 national survey, 88 percent of consumers said they were "concerned" by the amount of information being requested, including 55 percent who said they were "very concerned." See Privacy and American Business, 1998 Privacy Concerns & Consumer Choice Survey (<http://www.pandab.org>). These worries are not just theoretical. Consumers who use the Internet to make purchases or request "free" information often are asked for personal and financial information. Companies making such requests routinely promise to protect the confidentiality of that information. Yet several firms have tried to sell this information to other companies even after promising not to do so.

Americans' concern about the privacy of their health information is part of a broader anxiety about their lack of privacy in an array of areas. A series of national public opinion polls conducted by Louis Harris & Associates documents a rising level of public concern about privacy, growing from 64 percent in

1978 to 82 percent in 1995. Over 80 percent of persons surveyed in 1999 agreed with the statement that they had "lost all control over their personal information." See Harris Equifax, Health Information Privacy Study (1993) (<http://www.epic.org/privacy/medical/polls.html>). A Wall Street Journal/ABC poll on September 16, 1999 asked Americans what concerned them most in the coming century. "Loss of personal privacy" was the first or second concern of 29 percent of respondents. All other issues, such as terrorism, world war, and global warming had scores of 23 percent or less.

This growing concern stems from several trends, including the growing use of interconnected electronic media for business and personal activities, our increasing ability to know an individual's genetic make-up, and, in health care, the increasing complexity of the system. Each of these trends brings the potential for tremendous benefits to individuals and society generally. At the same time, each also brings new potential for invasions of our privacy.

#### *Increasing Use of Interconnected Electronic Information Systems*

Until recently, health information was recorded and maintained on paper and stored in the offices of community-based physicians, nurses, hospitals, and other health care professionals and institutions. In some ways, this imperfect system of record keeping created a false sense of privacy among patients, providers, and others. Patients' health information has never remained completely confidential. Until recently, however, a breach of confidentiality involved a physical exchange of paper records or a verbal exchange of information. Today, however, more and more health care providers, plans, and others are utilizing electronic means of storing and transmitting health information. In 1996, the health care industry invested an estimated \$10 billion to \$15 billion on information technology. See National Research Council, Computer Science and Telecommunications Board, "For the Record: Protecting Electronic Health Information," (1997). The electronic information revolution is transforming the recording of health information so that the disclosure of information may require only a push of a button. In a matter of seconds, a person's most profoundly private information can be shared with hundreds, thousands, even millions of individuals and organizations at a time. While the majority of medical records still are in paper form, information from those

records is often copied and transmitted through electronic means.

This ease of information collection, organization, retention, and exchange made possible by the advances in computer and other electronic technology affords many benefits to individuals and to the health care industry. Use of electronic information has helped to speed the delivery of effective care and the processing of billions of dollars worth of health care claims. Greater use of electronic data has also increased our ability to identify and treat those who are at risk for disease, conduct vital research, detect fraud and abuse, and measure and improve the quality of care delivered in the U.S. The National Research Council recently reported that "the Internet has great potential to improve Americans' health by enhancing communications and improving access to information for care providers, patients, health plan administrators, public health officials, biomedical researchers, and other health professionals." See "Networking Health: Prescriptions for the Internet," National Academy of Sciences (2000).

At the same time, these advances have reduced or eliminated many of the financial and logistical obstacles that previously served to protect the confidentiality of health information and the privacy interests of individuals. And they have made our information available to many more people. The shift from paper to electronic records, with the accompanying greater flows of sensitive health information, thus strengthens the arguments for giving legal protection to the right to privacy in health information. In an earlier period where it was far more expensive to access and use medical records, the risk of harm to individuals was relatively low. In the potential near future, when technology makes it almost free to send lifetime medical records over the Internet, the risks may grow rapidly. It may become cost-effective, for instance, for companies to offer services that allow purchasers to obtain details of a person's physical and mental treatments. In addition to legitimate possible uses for such services, malicious or inquisitive persons may download medical records for purposes ranging from identity theft to embarrassment to prurient interest in the life of a celebrity or neighbor. The comments to the proposed privacy rule indicate that many persons believe that they have a right to live in society without having these details of their lives laid open to unknown and possibly hostile eyes. These technological changes, in short, may provide a reason for institutionalizing

privacy protections in situations where the risk of harm did not previously justify writing such protections into law.

The growing level of trepidation about privacy in general, noted above, has tracked the rise in electronic information technology. Americans have embraced the use of the Internet and other forms of electronic information as a way to provide greater access to information, save time, and save money. For example, 60 percent of Americans surveyed in 1999 reported that they have a computer in their home; 82 percent reported that they have used a computer; 64 percent say they have used the Internet; and 58 percent have sent an e-mail. Among those who are under the age of 60, these percentages are even higher. See "National Survey of Adults on Technology," Henry J. Kaiser Family Foundation (February, 2000). But 59 percent of Americans reported that they worry that an unauthorized person will gain access to their information. A recent survey suggests that 75 percent of consumers seeking health information on the Internet are concerned or very concerned about the health sites they visit sharing their personal health information with a third party without their permission. Ethics Survey of Consumer Attitudes about Health Web Sites, California Health Care Foundation, at 3 (January, 2000).

Unless public fears are allayed, we will be unable to obtain the full benefits of electronic technologies. The absence of national standards for the confidentiality of health information has made the health care industry and the population in general uncomfortable about this primarily financially-driven expansion in the use of electronic data. Many plans, providers, and clearinghouses have taken steps to safeguard the privacy of individually identifiable health information. Yet they must currently rely on a patchwork of State laws and regulations that are incomplete and, at times, inconsistent. States have, to varying degrees, attempted to enhance confidentiality by establishing laws governing at least some aspects of medical record privacy. This approach, though a step in the right direction, is inadequate. These laws fail to provide a consistent or comprehensive legal foundation of health information privacy. For example, there is considerable variation among the states in the type of information protected and the scope of the protections provided. See Georgetown Study, at Executive Summary; Lawrence O. Gostin, Zita Lazzarini, Kathleen M. Flaherty,

Legislative Survey of State Confidentiality Laws, with Specific Emphasis on HIV and Immunization, Report to Centers for Disease Control, Council of State and Territorial Epidemiologists, and Task Force for Child Survival and Development, Carter Presidential Center (1996) (Gostin Study).

Moreover, electronic health data is becoming increasingly "national"; as more information becomes available in electronic form, it can have value far beyond the immediate community where the patient resides. Neither private action nor state laws provide a sufficiently comprehensive and rigorous legal structure to allay public concerns, protect the right to privacy, and correct the market failures caused by the absence of privacy protections (see discussion below of market failure under section V.C.). Hence, a national policy with consistent rules is necessary to encourage the increased and proper use of electronic information while also protecting the very real needs of patients to safeguard their privacy.

#### *Advances in Genetic Sciences*

Recently, scientists completed nearly a decade of work unlocking the mysteries of the human genome, creating tremendous new opportunities to identify and prevent many of the leading causes of death and disability in this country and around the world. Yet the absence of privacy protections for health information endanger these efforts by creating a barrier of distrust and suspicion among consumers. A 1995 national poll found that more than 85 percent of those surveyed were either "very concerned" or "somewhat concerned" that insurers and employers might gain access to and use genetic information. See Harris Poll, 1995 #34. Sixty-three percent of the 1,000 participants in a 1997 national survey said they would not take genetic tests if insurers and employers could gain access to the results. See "Genetic Information and the Workplace," Department of Labor, Department of Health and Human Services, Equal Employment Opportunity Commission, January 20, 1998. "In genetic testing studies at the National Institutes of Health, thirty-two percent of eligible people who were offered a test for breast cancer risk declined to take it, citing concerns about loss of privacy and the potential for discrimination in health insurance." Sen. Leahy's comments for March 10, 1999 Introduction of the Medical Information Privacy and Security Act.

#### *The Changing Health Care System*

The number of entities who are maintaining and transmitting individually identifiable health information has increased significantly over the last 10 years. In addition, the rapid growth of integrated health care delivery systems requires greater use of integrated health information systems. The health care industry has been transformed from one that relied primarily on one-on-one interactions between patients and clinicians to a system of integrated health care delivery networks and managed care providers. Such a system requires the processing and collection of information about patients and plan enrollees (for example, in claims files or enrollment records), resulting in the creation of databases that can be easily transmitted. This dramatic change in the practice of medicine brings with it important prospects for the improvement of the quality of care and reducing the cost of that care. It also, however, means that increasing numbers of people have access to health information. And, as health plan functions are increasingly outsourced, a growing number of organizations not affiliated with our physicians or health plans also have access to health information.

According to the American Health Information Management Association (AHIMA), an average of 150 people "from nursing staff to x-ray technicians, to billing clerks" have access to a patient's medical records during the course of a typical hospitalization. While many of these individuals have a legitimate need to see all or part of a patient's records, no laws govern who those people are, what information they are able to see, and what they are and are not allowed to do with that information once they have access to it. According to the National Research Council, individually identifiable health information frequently is shared with:

- Consulting physicians;
- Managed care organizations;
- Health insurance companies;
- Life insurance companies;
- Self-insured employers;
- Pharmacies;
- Pharmacy benefit managers;
- Clinical laboratories;
- Accrediting organizations;
- State and Federal statistical agencies; and
- Medical information bureaus.

Much of this sharing of information is done without the knowledge of the patient involved. While many of these functions are important for smooth functioning of the health care system, there are no rules governing how that

information is used by secondary and tertiary users. For example, a pharmacy benefit manager could receive information to determine whether an insurance plan or HMO should cover a prescription, but then use the information to market other products to the same patient. Similarly, many of us obtain health insurance coverage through our employer and, in some instances, the employer itself acts as the insurer. In these cases, the employer will obtain identifiable health information about its employees as part of the legitimate health insurance functions such as claims processing, quality improvement, and fraud detection activities. At the same time, there is no comprehensive protection prohibiting the employer from using that information to make decisions about promotions or job retention.

Public concerns reflect these developments. A 1993 Lou Harris poll found that 75 percent of those surveyed worry that medical information from a computerized national health information system will be used for many non-health reasons, and 38 percent are very concerned. This poll, taken during the health reform efforts of 1993, showed that 85 percent of respondents believed that protecting the confidentiality of medical records is "absolutely essential" or "very essential" in health care reform. An ACLU Poll in 1994 also found that 75 percent of those surveyed are concerned a "great deal" or a "fair amount" about insurance companies putting medical information about them into a computer information bank to which others have access. Harris Equifax, Health Information Privacy Study 2,33 (1993) <http://www.epic.org/privacy/medical/poll.html>. Another survey found that 35 percent of Fortune 500 companies look at people's medical records before making hiring and promotion decisions. Starr, Paul. "Health and the Right to Privacy," American Journal of Law and Medicine, 1999, Vol 25, pp. 193-201.

Concerns about the lack of attention to information privacy in the health care industry are not merely theoretical. In the absence of a national legal framework of health privacy protections, consumers are increasingly vulnerable to the exposure of their personal health information. Disclosure of individually identifiable information can occur deliberately or accidentally and can occur within an organization or be the result of an external breach of security. Examples of recent privacy breaches include:

- A Michigan-based health system accidentally posted the medical records of thousands of patients on the Internet

(The Ann Arbor News, February 10, 1999).

- A Utah-based pharmaceutical benefits management firm used patient data to solicit business for its owner, a drug store (Kiplingers, February 2000).

- An employee of the Tampa, Florida, health department took a computer disk containing the names of 4,000 people who had tested positive for HIV, the virus that causes AIDS (USA Today, October 10, 1996).

- The health insurance claims forms of thousands of patients blew out of a truck on its way to a recycling center in East Hartford, Connecticut (The Hartford Courant, May 14, 1999).

- A patient in a Boston-area hospital discovered that her medical record had been read by more than 200 of the hospital's employees (The Boston Globe, August 1, 2000).

- A Nevada woman who purchased a used computer discovered that the computer still contained the prescription records of the customers of the pharmacy that had previously owned the computer. The pharmacy data base included names, addresses, social security numbers, and a list of all the medicines the customers had purchased. (The New York Times, April 4, 1997 and April 12, 1997).

- A speculator bid \$4000 for the patient records of a family practice in South Carolina. Among the businessman's uses of the purchased records was selling them back to the former patients. (New York Times, August 14, 1991).

- In 1993, the Boston Globe reported that Johnson and Johnson marketed a list of 5 million names and addresses of elderly incontinent women. (ACLU Legislative Update, April 1998).

- A few weeks after an Orlando woman had her doctor perform some routine tests, she received a letter from a drug company promoting a treatment for her high cholesterol. (Orlando Sentinel, November 30, 1997).

No matter how or why a disclosure of personal information is made, the harm to the individual is the same. In the face of industry evolution, the potential benefits of our changing health care system, and the real risks and occurrences of harm, protection of privacy must be built into the routine operations of our health care system.

#### *Privacy Is Necessary To Secure Effective, High Quality Health Care*

While privacy is one of the key values on which our society is built, it is more than an end in itself. It is also necessary for the effective delivery of health care, both to individuals and to populations. The market failures caused by the lack

of effective privacy protections for health information are discussed below (see section V.C below). Here, we discuss how privacy is a necessary foundation for delivery of high quality health care. In short, the entire health care system is built upon the willingness of individuals to share the most intimate details of their lives with their health care providers.

The need for privacy of health information, in particular, has long been recognized as critical to the delivery of needed medical care. More than anything else, the relationship between a patient and a clinician is based on trust. The clinician must trust the patient to give full and truthful information about their health, symptoms, and medical history. The patient must trust the clinician to use that information to improve his or her health and to respect the need to keep such information private. In order to receive accurate and reliable diagnosis and treatment, patients must provide health care professionals with accurate, detailed information about their personal health, behavior, and other aspects of their lives. The provision of health information assists in the diagnosis of an illness or condition, in the development of a treatment plan, and in the evaluation of the effectiveness of that treatment. In the absence of full and accurate information, there is a serious risk that the treatment plan will be inappropriate to the patient's situation.

Patients also benefit from the disclosure of such information to the health plans that pay for and can help them gain access to needed care. Health plans and health care clearinghouses rely on the provision of such information to accurately and promptly process claims for payment and for other administrative functions that directly affect a patient's ability to receive needed care, the quality of that care, and the efficiency with which it is delivered.

Accurate medical records assist communities in identifying troubling public health trends and in evaluating the effectiveness of various public health efforts. Accurate information helps public and private payers make correct payments for care received and lower costs by identifying fraud. Accurate information provides scientists with data they need to conduct research. We cannot improve the quality of health care without information about which treatments work, and which do not.

Individuals cannot be expected to share the most intimate details of their lives unless they have confidence that such information will not be used or

shared inappropriately. Privacy violations reduce consumers' trust in the health care system and institutions that serve them. Such a loss of faith can impede the quality of the health care they receive, and can harm the financial health of health care institutions.

Patients who are worried about the possible misuse of their information often take steps to protect their privacy. Recent studies show that a person who does not believe his privacy will be protected is much less likely to participate fully in the diagnosis and treatment of his medical condition. A national survey conducted in January 1999 found that one in five Americans believe their health information is being used inappropriately. See California HealthCare Foundation, "National Survey: Confidentiality of Medical Records" (January, 1999) (<http://www.chcf.org>). More troubling is the fact that one in six Americans reported that they have taken some sort of evasive action to avoid the inappropriate use of their information by providing inaccurate information to a health care provider, changing physicians, or avoiding care altogether. Similarly, in its comments on our proposed rule, the Association of American Physicians and Surgeons reported 78 percent of its members reported withholding information from a patient's record due to privacy concerns and another 87 percent reported having had a patient request to withhold information from their records. For an example of this phenomenon in a particular demographic group, see Drs. Bearman, Ford, and Moody, "Foregone Health Care among Adolescents," *JAMA*, vol. 282, no. 23 (1999); Cheng, T.L., et al., "Confidentiality in Health Care: A Survey of Knowledge, Perceptions, and Attitudes among High School Students," *JAMA*, vol. 269, no. 11 (1993); at 1404-1407.

The absence of strong national standards for medical privacy has widespread consequences. Health care professionals who lose the trust of their patients cannot deliver high-quality care. In 1999, a coalition of organizations representing various stakeholders including health plans, physicians, nurses, employers, disability and mental health advocates, accreditation organizations as well as experts in public health, medical ethics, information systems, and health policy adopted a set of "best principles" for health care privacy that are consistent with the standards we lay out here. (See the Health Privacy Working Group, "Best Principles for Health Privacy"

(July, 1999) (Best Principles Study). The Best Principles Study states that—

To protect their privacy and avoid embarrassment, stigma, and discrimination, some people withhold information from their health care providers, provide inaccurate information, doctor-hop to avoid a consolidated medical record, pay out-of-pocket for care that is covered by insurance, and—in some cases—avoid care altogether.

Best Principles Study, at 9. In their comments on our proposed rule, numerous organizations representing health plans, health providers, employers, and others acknowledged the value of a set of national privacy standards to the efficient operation of their practices and businesses.

#### *Breaches of Health Privacy Harm More Than Our Health Status*

A breach of a person's health privacy can have significant implications well beyond the physical health of that person, including the loss of a job, alienation of family and friends, the loss of health insurance, and public humiliation. For example:

- A banker who also sat on a county health board gained access to patients' records and identified several people with cancer and called in their mortgages. See the *National Law Journal*, May 30, 1994.
- A physician was diagnosed with AIDS at the hospital in which he practiced medicine. His surgical privileges were suspended. See *Estate of Behringer v. Medical Center at Princeton*, 249 N.J. Super. 597.
- A candidate for Congress nearly saw her campaign derailed when newspapers published the fact that she had sought psychiatric treatment after a suicide attempt. See *New York Times*, October 10, 1992, Section 1, page 25.

• A 30-year FBI veteran was put on administrative leave when, without his permission, his pharmacy released information about his treatment for depression. (*Los Angeles Times*, September 1, 1998) Consumer Reports found that 40 percent of insurers disclose personal health information to lenders, employers, or marketers without customer permission. "Who's reading your Medical Records," *Consumer Reports*, October 1994, at 628, paraphrasing Sweeny, Latanya, "Weaving Technology and Policy Together to Maintain Confidentiality," *The Journal Of Law Medicine and Ethics* (Summer & Fall 1997) Vol. 25, Numbers 2,3.

The answer to these concerns is not for consumers to withdraw from society and the health care system, but for society to establish a clear national legal framework for privacy. By spelling out

what is and what is not an allowable use of a person's identifiable health information, such standards can help to restore and preserve trust in the health care system and the individuals and institutions that comprise that system. As medical historian Paul Starr wrote: "Patients have a strong interest in preserving the privacy of their personal health information but they also have an interest in medical research and other efforts by health care organizations to improve the medical care they receive. As members of the wider community, they have an interest in public health measures that require the collection of personal data." (P. Starr, "Health and the Right to Privacy," *American Journal of Law & Medicine*, 25, nos. 2&3 (1999) 193-201). The task of society and its government is to create a balance in which the individual's needs and rights are balanced against the needs and rights of society as a whole.

National standards for medical privacy must recognize the sometimes competing goals of improving individual and public health, advancing scientific knowledge, enforcing the laws of the land, and processing and paying claims for health care services. This need for balance has been recognized by many of the experts in this field. Cavoukian and Tapscott described it this way: "An individual's right to privacy may conflict with the collective rights of the public \* \* \*. We do not suggest that privacy is an absolute right that reigns supreme over all other rights. It does not. However, the case for privacy will depend on a number of factors that can influence the balance—the level of harm to the individual involved versus the needs of the public."

#### *The Federal Response*

There have been numerous federal initiatives aimed at protecting the privacy of especially sensitive personal information over the past several years—and several decades. While the rules below are likely the largest single federal initiative to protect privacy, they are by no means alone in the field. Rather, the rules arrive in the context of recent legislative activity to grapple with advances in technology, in addition to an already established body of law granting federal protections for personal privacy.

In 1965, the House of Representatives created a Special Subcommittee on Invasion of Privacy. In 1973, this Department's predecessor agency, the Department of Health, Education and Welfare issued The Code of Fair Information Practice Principles establishing an important baseline for

information privacy in the U.S. These principles formed the basis for the federal Privacy Act of 1974, which regulates the government's use of personal information by limiting the disclosure of personally-identifiable information, allows consumers access to information about them, requires federal agencies to specify the purposes for collecting personal information, and provides civil and criminal penalties for misuse of information.

In the last several years, with the rapid expansion in electronic technology—and accompanying concerns about individual privacy—laws, regulations, and legislative proposals have been developed in areas ranging from financial privacy to genetic privacy to the safeguarding of children on-line. For example, the Children's Online Privacy Protection Act was enacted in 1998, providing protection for children when interacting at websites. In February, 2000, President Clinton signed Executive Order 13145, banning the use of genetic information in federal hiring and promotion decisions. The landmark financial modernization bill, signed by the President in November, 1999, likewise contained financial privacy protections for consumers. There also has been recent legislative activity on establishing legal safeguards for the privacy of individuals' Social Security numbers, and calls for regulation of on-line privacy in general.

These most recent laws, regulations, and legislative proposals come against the backdrop of decades of privacy-enhancing statutes passed at the federal level to enact safeguards in fields ranging from government data files to video rental records. In the 1970s, individual privacy was paramount in the passage of the Fair Credit Reporting Act (1970), the Privacy Act (1974), the Family Educational Rights and Privacy Act (1974), and the Right to Financial Privacy Act (1978). These key laws were followed in the next decade by another series of statutes, including the Privacy Protection Act (1980), the Electronic Communications Privacy Act (1986), the Video Privacy Protection Act (1988), and the Employee Polygraph Protection Act (1988). In the last ten years, Congress and the President have passed additional legal privacy protection through, among others, the Telephone Consumer Protection Act (1991), the Driver's Privacy Protection Act (1994), the Telecommunications Act (1996), the Children's Online Privacy Protection Act (1998), the Identity Theft and Assumption Deterrence Act (1998), and Title V of the Gramm-Leach-Bliley Act (1999) governing financial privacy.

In 1997, a Presidential advisory commission, the Advisory Commission on Consumer Protection and Quality in the Health Care Industry, recognized the need for patient privacy protection in its recommendations for a Consumer Bill of Rights and Responsibilities (November 1997). In 1997, Congress enacted the Balanced Budget Act (Public Law 105-34), which added language to the Social Security Act (18 U.S.C. 1852) to require Medicare+Choice organizations to establish safeguards for the privacy of individually identifiable patient information. Similarly, the Veterans Benefits section of the U.S. Code provides for confidentiality of medical records in cases involving drug abuse, alcoholism or alcohol abuse, HIV infection, or sickle cell anemia (38 U.S.C. 7332).

As described in more detail in the next section, Congress recognized the importance of protecting the privacy of health information by enacting the Health Insurance Portability and Accountability Act of 1996. The Act called on Congress to enact a medical privacy statute and asked the Secretary of Health and Human Services to provide Congress with recommendations for protecting the confidentiality of health care information. The Congress further recognized the importance of such standards by providing the Secretary with authority to promulgate regulations on health care privacy in the event that lawmakers were unable to act within the allotted three years.

Finally, it also is important for the U.S. to join the rest of the developed world in establishing basic medical privacy protections. In 1995, the European Union (EU) adopted a Data Privacy Directive requiring its 15 member states to adopt consistent privacy laws by October 1998. The EU urged all other nations to do the same or face the potential loss of access to information from EU countries.

#### *Statutory Background*

#### *History of the Privacy Component of the Administrative Simplification Provisions*

The Congress addressed the opportunities and challenges presented by the rapid evolution of health information systems in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, which was enacted on August 21, 1996. Sections 261 through 264 of HIPAA are known as the Administrative Simplification provisions. The major part of these Administrative Simplification

provisions are found at section 262 of HIPAA, which enacted a new part C of title XI of the Social Security Act (hereinafter we refer to the Social Security Act as the "Act" and we refer to all other laws cited in this document by their names).

In section 262, Congress primarily sought to facilitate the efficiencies and cost savings for the health care industry that the increasing use of electronic technology affords. Thus, section 262 directs HHS to issue standards to facilitate the electronic exchange of information with respect to financial and administrative transactions carried out by health plans, health care clearinghouses, and health care providers who transmit information electronically in connection with such transactions.

At the same time, Congress recognized the challenges to the confidentiality of health information presented by the increasing complexity of the health care industry, and by advances in health information systems technology and communications. Section 262 thus also directs HHS to develop standards to protect the security, including the confidentiality and integrity, of health information.

Congress has long recognized the need for protection of health information privacy generally, as well as the privacy implications of electronic data interchange and the increased ease of transmitting and sharing individually identifiable health information. Congress has been working on broad health privacy legislation for many years and, as evidenced by the self-imposed three year deadline included in the HIPAA, discussed below, believes it can and should enact such legislation. A significant portion of the first Administrative Simplification section debated on the floor of the Senate in 1994 (as part of the Health Security Act) consisted of privacy provisions. In the version of the HIPAA passed by the House of Representatives in 1996, the requirement for the issuance of privacy standards was located in the same section of the bill (section 1173) as the requirements for issuance of the other HIPAA Administrative Simplification standards. In conference, the requirement for privacy standards was moved to a separate section in the same part of HIPAA, section 264, so that Congress could link the Privacy standards to Congressional action.

Section 264(b) requires the Secretary of HHS to develop and submit to the Congress recommendations for:

- The rights that an individual who is a subject of individually identifiable health information should have.

- The procedures that should be established for the exercise of such rights.
- The uses and disclosures of such information that should be authorized or required.

The Secretary's Recommendations were submitted to the Congress on September 11, 1997. Section 264(c)(1) provides that:

If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by [August 21, 1999], the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than [February 21, 2000]. Such regulations shall address at least the subjects described in subsection (b).

As the Congress did not enact legislation regarding the privacy of individually identifiable health information prior to August 21, 1999, HHS published proposed rules setting forth such standards on November 3, 1999, 64 FR 59918, and is now publishing the mandated final regulation.

These privacy standards have been, and continue to be, an integral part of the suite of Administrative Simplification standards intended to simplify and improve the efficiency of the administration of our health care system.

#### *The Administrative Simplification Provisions, and Regulatory Actions to Date*

Part C of title XI consists of sections 1171 through 1179 of the Act. These sections define various terms and impose several requirements on HHS, health plans, health care clearinghouses, and health care providers who conduct the identified transactions electronically.

The first section, section 1171 of the Act, establishes definitions for purposes of part C of title XI for the following terms: code set, health care clearinghouse, health care provider, health information, health plan, individually identifiable health information, standard, and standard setting organization.

Section 1172 of the Act makes the standard adopted under part C applicable to: (1) Health plans, (2) health care clearinghouses, and (3) health care providers who transmit health information in electronic form in connection with transactions referred to in section 1173(a)(1) of the Act (hereinafter referred to as the "covered entities"). Section 1172 also contains

procedural requirements concerning the adoption of standards, including the role of standard setting organizations and required consultations, summarized in subsection F and section VI, below.

Section 1173 of the Act requires the Secretary to adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically. Section 1173(a)(1) describes the transactions to be promulgated, which include the nine transactions listed in section 1173(a)(2) and other transactions determined appropriate by the Secretary. The remainder of section 1173 sets out requirements for the specific standards the Secretary is to adopt: Unique health identifiers, code sets, security standards, electronic signatures, and transfer of information among health plans. Of particular relevance to this proposed rule is section 1173(d), the security standard provision. The security standard authority applies to both the transmission and the maintenance of health information, and requires the entities described in section 1172(a) to maintain reasonable and appropriate safeguards to ensure the integrity and confidentiality of the information, protect against reasonably anticipated threats or hazards to the security or integrity of the information or unauthorized uses or disclosures of the information, and to ensure compliance with part C by the entity's officers and employees.

In section 1174 of the Act, the Secretary is required to establish standards for all of the above transactions, except claims attachments, by February 21, 1998. The statutory deadline for the claims attachment standard is February 21, 1999.

As noted above, a proposed rule for most of the transactions was published on May 7, 1998, and the final Transactions Rule was promulgated on August 17, 2000. The delay was caused by the deliberate consensus building process, working with industry, and the large number of comments received (about 17,000). In addition, in a series of Notices of Proposed Rulemakings, HHS published other proposed standards, as described above. Each of these steps was taken in concert with the affected professions and industries, to ensure rapid adoption and compliance.

Generally, after a standard is established, it may not be changed during the first year after adoption except for changes that are necessary to permit compliance with the standard. Modifications to any of these standards may be made after the first year, but not

more frequently than once every 12 months. The Secretary also must ensure that procedures exist for the routine maintenance, testing, enhancement, and expansion of code sets and that there are crosswalks from prior versions.

Section 1175 of the Act prohibits health plans from refusing to process, or from delaying processing of, a transaction that is presented in standard format. It also establishes a timetable for compliance: each person to whom a standard or implementation specification applies is required to comply with the standard within 24 months (or 36 months for small health plans) of its adoption. A health plan or other entity may, of course, comply voluntarily before the effective date. The section also provides that compliance with modifications to standards or implementation specifications must be accomplished by a date designated by the Secretary, which date may not be earlier than 180 days from the notice of change.

Section 1176 of the Act establishes civil monetary penalties for violation of the provisions in part C of title XI of the Act, subject to several limitations. Penalties may not be more than \$100 per person per violation and not more than \$25,000 per person for violations of a single standard for a calendar year. The procedural provisions of section 1128A of the Act apply to actions taken to obtain civil monetary penalties under this section.

Section 1177 establishes penalties for any person that knowingly uses a unique health identifier, or obtains or discloses individually identifiable health information in violation of the part. The penalties include: (1) A fine of not more than \$50,000 and/or imprisonment of not more than 1 year; (2) if the offense is "under false pretenses," a fine of not more than \$100,000 and/or imprisonment of not more than 5 years; and (3) if the offense is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than \$250,000 and/or imprisonment of not more than 10 years.

Under section 1178 of the Act, the requirements of part C, as well as any standards or implementation specifications adopted thereunder, preempt contrary state law. There are three exceptions to this general rule of preemption: State laws that the Secretary determines are necessary for certain purposes set forth in the statute; state laws that the Secretary determines address controlled substances; and state laws relating to the privacy of

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF WISCONSIN**

**Electronic Case Filing ("ECF")**

**PROCEDURAL ORDER**

**Introduction**

Federal Rules of Civil Procedure 5(e) authorizes this Court to establish practices and procedures for the filing, signing and verification of documents by electronic means. All civil and criminal cases filed on or after October 1, 2003, will be designated for Electronic Case Filing (ECF). The only exclusions from ECF shall be: criminal juvenile cases and cases filed by either a prisoner or a pro se party. The following procedures apply to all cases designated for ECF:

**1. Scope of Electronic Filing**

Those civil and criminal cases filed in this court on or after October 1, 2003, and designated for ECF, will be entered into the court's ECF system in accordance with this Procedural Order on Electronic Case Filing ("Procedural Order"). Except as expressly provided in this Procedural Order, all petitions, motions, memoranda of law, or other pleadings and documents required to be filed with the court in connection with an ECF assigned case, will be maintained in electronic format.

The filing of all initial papers in civil cases, such as the complaint and the issuance and service of the summons, and in criminal cases, the indictment or information, warrant for arrest or summons, will be accomplished in the traditional manner on paper rather than electronically. If the case is assigned to the ECF system, these filed documents will be converted to electronic format.

**2. Eligibility, Registration, Passwords**

Attorneys admitted to the bar of this court, including those admitted pro hac vice, may register as ECF Users of the Court's ECF system. Registration is in a form prescribed by the clerk and requires the ECF User's name, address, telephone number, Internet e-mail address, and a declaration that the attorney is admitted to the bar of this court and is a member in good standing.

Registration as an ECF User constitutes agreement to receive and consent to make electronic service of all documents as provided in this Procedural Order in accordance with Rule 5(b)(2)(D) of the Federal Rules of Civil Procedure and in Rule 49(b) of the Federal Rules of Criminal Procedure. This agreement and consent is applicable to all future cases until revoked by the ECF User.

Once registration is completed, the ECF User will receive notification of the user login and password. ECF Users agree to protect the security of their passwords and immediately notify the clerk if they learn that their password has been compromised. ECF Users may be subject to sanctions for failure to comply with this provision.

No ECF User shall knowingly permit or cause to permit his or her login and password to be used by anyone other than an authorized employee of his or her law firm or organization.

### **3. Consequences of Electronic Filing**

Electronic transmission of a document to the ECF system consistent with this Procedural Order, together with the transmission of a Notice of Electronic Filing from the court, constitutes filing of the document for all purposes of the Federal Rules of Civil Procedure, the Federal Rules of Criminal Procedure, and the Local Rules of this court, and constitutes entry of the document on the docket maintained by the clerk pursuant to Rules 58 and 79 of the Federal Rules of Civil Procedure and Rules 49 and 55 of the Federal Rules of Criminal Procedure.

A document that has been filed electronically is the official record, and the filing party is bound by the document as filed. Except in the case of documents first filed in paper form and subsequently submitted electronically under Section 1 above, a document filed electronically is deemed filed at the date and time stated on the Notice of Electronic Filing from the court.

Filing a document electronically does not change any filing deadline set by the Federal Rules of Civil Procedure, the Federal Rules of Criminal Procedure, the Local Rules of this court, or an order of the judge.

Documents filed electronically must be submitted in PDF format. Documents which the filer has in an electronic format other than PDF must be converted to PDF from the word processing original, not scanned, to facilitate transmission and retrieval. Only documents of which the filer possesses only a paper copy may be scanned to convert them to PDF format.

### **4. Entry of Court Orders**

All orders, decrees, judgments, and proceedings of the court will be filed in accordance with these rules which will constitute entry on the docket kept by the clerk under Rules 58 and 79 of the Federal Rules of Civil Procedure, and Rules 49 and 55 of the Federal Rules of Criminal Procedure. All signed orders will be filed electronically by the court or court personnel. Any order filed electronically without the original signature of a judge has the same force and effect as if the judge had affixed the judge's signature to a paper copy of the order and it had been entered on the docket in a conventional manner.

An ECF User submitting a document electronically that requires a judge's signature must promptly deliver the document in such form as the court requires.

### **5. Attachments and Exhibits**

ECF Users must submit in electronic form all documents referenced as attachments or exhibits, unless the court permits conventional filing. An ECF User must submit as attachments or exhibits only those excerpts of the referenced documents that are directly germane to the matter under consideration by the court. Excerpted material must be clearly and prominently identified as such. ECF Users who file excerpts of documents as attachments or exhibits pursuant to this Procedural

Order, do so without prejudice to their right to timely file additional excerpts or the complete document, provided however, that the size of the document does not exceed two megabytes. Attachments or exhibits exceeding two megabytes may be broken down into separate sections, each not exceeding two megabytes, or filed on paper in the traditional manner. Responding parties who choose to file attachments or exhibits electronically may also timely file additional excerpts or the complete document, subject to the same size limitations as set forth above.

## **6. Retention Requirements**

Documents that are electronically filed and require original signatures other than that of the ECF User must be maintained in paper form by the ECF User until one year has passed after the time period for appeal expires. The ECF User must provide original documents for review upon request of the judge.

## **7. Signatures**

The user login and password required to submit documents to the ECF system serve as the ECF User's signature on all electronic documents filed with the court. They also serve as a signature for purposes of Rule 11(a) of the Federal Rules of Civil Procedure and any other purpose for which a signature is required in connection with proceedings before the court. Electronically filed documents must include a signature block and must set forth the name, address, telephone number and the attorney's state bar registration number, if applicable. In addition, the name of the ECF User under whose login and password the document is submitted must be preceded by an "s/" and typed in the space where the signature would otherwise appear.

Documents requiring multiple signatures, such as stipulations, shall be electronically filed as follows: (1) the ECF User shall obtain the signatures of all parties on the document; (2) the ECF User shall electronically file the document indicating the signatories in the format as described above; and (3) a non-filing signatory or party who disputes the authenticity of an electronically filed document containing multiple signatures must file an objection to the document within ten days of receiving the Notice of Electronic Filing.

## **8. Service of Documents by Electronic Means**

When an ECF User electronically files a pleading or other document using the ECF system, a Notice of Electronic Filing shall automatically be generated by the system, and shall be sent automatically to all parties entitled to service under the Federal Rules of Civil Procedure and the Federal Rules of Criminal Procedure and who have consented to electronic service. Electronic service of the Notice of Electronic Filing constitutes service of the filed document to all such parties and shall be deemed to satisfy the requirements of Rule 5(b)(2)(D) of the Federal Rules of Civil Procedure and Rule 49(b) of the Federal Rules of Criminal Procedure.

All documents filed using the ECF system shall contain a Certificate of Service stating that the document has been filed electronically and is available for viewing and downloading from the ECF system. The Certificate of Service must identify the manner in which service on each party was accomplished, including any party who has not consented to electronic service.

Parties who have not consented to electronic service are entitled to receive a paper copy of any electronically filed pleading or other document. Service of such paper copy must be made according to the Federal Rules of Civil Procedure and the Federal Rules of Criminal Procedure.

In accordance with Rule 6(e) of the Federal Rules of Civil Procedure, service by electronic means is treated the same as service by mail.

## **9. Technical Failures**

A filing party whose filing is made untimely as the result of the technical failure of the court's ECF system may seek appropriate relief from the presiding judge.

## **10. Public Access**

The Office of the Clerk is now accepting electronically filed pleadings and making the content of these pleadings available on the court's Internet website via WebPACER. Any subscriber to WebPACER will be able to read, download, store and print the full content of electronically filed documents. The clerk's office will not make electronically available documents that have been sealed or otherwise restricted by court order.

Any person or organization, other than one registered as an ECF User under Section 2 of this Procedural Order, may access ECF at the court's Internet site, [www.wied.uscourts.gov](http://www.wied.uscourts.gov), by obtaining a PACER login and password. Those who have PACER access, but who are not ECF Users, may retrieve docket sheets and those documents which the court makes available on the Internet for the fee normally charged for this service as set by the fee schedule authorized by the Administrative Office of the United States Courts, but they may not file documents.

With the exception of Social Security Appeals, documents in civil cases will be made available electronically to the same extent that they are available for personal inspection in the Office of the Clerk of Court at the U.S. Courthouse. Public remote access to documents in Social Security Appeals and to documents in criminal cases will be limited to attorneys of record

In compliance with the E-Government Act of 2002, a party wishing to file a document containing the personal data identifiers specified below in an ECF case, may file an unredacted document under seal. This document shall be retained by the court as part of the record. The court may, however, still require the party to file a redacted copy for the public file.

Exercise caution when filing documents in an ECF case that contain the following:

- 1) Social Security numbers
- 2) financial account numbers
- 3) dates of birth
- 4) names of minor children
- 5) personal identifying numbers, such as a driver's license number
- 6) medical records, treatment and diagnosis
- 7) employment history

- 8) individual financial information
- 9) proprietary or trade secret information

Counsel is strongly urged to share this notice with all clients so that an informed decision about the inclusion of certain materials may be made. **The clerk will not review each pleading for redaction.**

#### **11. Record on Appeal**

Until such time as the United States Court of Appeals for the 7th Circuit and the Federal Circuit institute rules and procedures to accommodate ECF, notices of appeal to those courts shall be filed, and fees paid, in the traditional manner on paper rather than electronically. All further documents relating to the appeal shall be filed pursuant to the Federal Rules of Appellate Procedure and the Local Rules of the 7th Circuit. Appellant's counsel shall provide paper copies of the documents that constitute the record on appeal to the District Court Clerk's Office.

#### **12. Excluded Documents and Cases**

The following types of documents and categories of cases are presently excluded from the provisions of this Procedural Order. This list may be amended from time to time.

##### Excluded Documents

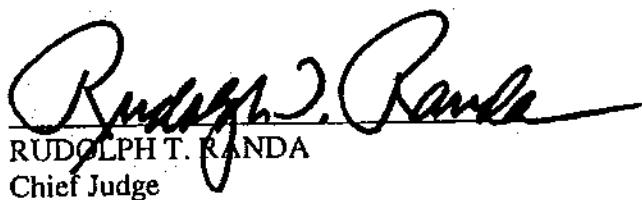
Civil Complaint  
Criminal Indictment or Information  
Notice of Appeal  
Criminal Plea Agreement  
State Court Records  
Social Security Transcripts  
Bankruptcy Appeal Transcripts  
Documents exceeding two megabytes  
Documents unavailable in ECF format

##### Excluded Cases

Criminal Juvenile  
Prisoner  
Pro se

**IT IS SO ORDERED.**

Dated at Milwaukee, Wisconsin, this 29th day of September, 2003.



RUDOLPH T. RANDA  
Chief Judge

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF WISCONSIN**

**Electronic Case Filing ("ECF")**

**PROCEDURAL ORDER  
AMENDED DECEMBER 1, 2007**

**Introduction**

Federal Rules of Civil Procedure 5(e) authorizes this Court to establish practices and procedures for the filing, signing and verification of documents by electronic means. All civil and criminal cases filed on or after October 1, 2003, will be designated for Electronic Case Filing (ECF). The only exclusions from ECF shall be criminal juvenile cases. The following procedures apply to all cases designated for ECF:

**1. Scope of Electronic Filing**

Those civil and criminal cases filed in this court on or after October 1, 2003, and designated for ECF, will be entered into the court's ECF system in accordance with this Procedural Order on Electronic Case Filing ("Procedural Order"). Except as expressly provided in the Procedural Order, all petitions, motions, memoranda of law, or other pleadings and documents required to be filed with the court in connection with an ECF assigned case, will be maintained in electronic format.

The filing of all initial papers in civil cases, such as the complaint and the issuance and service of the summons, and in criminal cases, the indictment or information, warrant for arrest or summons, will be accomplished in the traditional manner on paper and subsequently converted to electronic format.

**2. Eligibility, Registration, Passwords**

Attorneys admitted to the bar of this court may register as ECF Users of the Court's ECF system. Registration is in a form prescribed by the clerk and requires the ECF User's name, address, telephone number, Internet e-mail address, and a declaration that the attorney is admitted to the bar of this court and is a member in good standing.

Registration as an ECF User constitutes agreement to receive and consent to make electronic service of all documents as provided in this Procedural Order in accordance with Rule 5(b)(2)(D) of the Federal Rules of Civil Procedure and in Rule 49(b) of the Federal Rules of Criminal Procedure. This agreement and consent is applicable to all future cases until revoked by the ECF User.



Once registration is completed, the ECF User will receive notification of the user login and password. ECF Users agree to protect the security of their passwords and immediately notify the clerk if they learn that their password has been compromised. ECF Users may be subject to sanctions for failure to comply with this provision.

No ECF User shall knowingly permit or cause to permit his or her login and password to be used by anyone other than an authorized employee of his or her law firm or organization.

### **3. Consequences of Electronic Filing**

Electronic transmission of a document to the ECF system consistent with this Procedural Order, together with the transmission of a Notice of Electronic Filing from the court, constitutes filing of the document for all purposes of the Federal Rules of Civil Procedure, the Federal Rules of Criminal Procedure, and the Local Rules of this court, and constitutes entry of the document on the docket maintained by the clerk pursuant to Rules 58 and 79 of the Federal Rules of Civil Procedure and Rules 49 and 55 of the Federal Rules of Criminal Procedure.

A document that has been filed electronically is the official record, and the filing party is bound by the document as filed. Except in the case of documents first filed in paper form and subsequently converted to electronic format under Section 1 above, a document filed electronically is deemed filed at the date and time stated on the Notice of Electronic Filing from the court.

Filing a document electronically does not change any filing deadlines set by the Federal Rules of Civil Procedure, the Federal Rules of Criminal Procedure, the Local Rules of this court, or an order of the judge.

Documents filed electronically must be submitted in PDF format. Documents which the filer has in an electronic format other than PDF must be converted to PDF from the word processing original. Documents of which the filer possesses only a paper copy may be scanned to convert them to PDF Format.

### **4. Entry of Court Orders**

All orders, decrees, judgments, and proceedings of the court will be filed in accordance with these rules which will constitute entry on the docket kept by the clerk under Rules 58 and 79 of the Federal Rules of Civil Procedure, and Rules 49 and 55 of the Federal Rules of Criminal Procedure. All signed orders will be filed electronically by the court or court personnel. Any order filed electronically without the original signature of a judge has the same force and effect as if the judge had affixed the judge's signature to a paper copy of the order and it had been entered on the docket in a conventional manner.

An ECF User submitting a document electronically that requires a judge's signature must promptly deliver the document in such form as the court requires.

## **5. Attachments and Exhibits**

ECF Users must submit in electronic form all documents referenced as attachments or exhibits, unless the court permits conventional filing. An ECF User must submit as attachments or exhibits only those excerpts of the referenced documents that are directly germane to the matter under consideration by the court. Excerpted material must be clearly and prominently identified as such. ECF Users who file excerpts of documents as attachments or exhibits pursuant to this Procedural Order, do so without prejudice to the right to timely file additional excerpts or the complete document, provided however, that the size of the document does not exceed five megabytes. Attachments or exhibits exceeding five megabytes may be broken down into separate sections, each not exceeding five megabytes, or filed on paper in the traditional manner. Responding parties who choose to file attachments or exhibits electronically may also timely file additional excerpts or the complete document, subject to the same size limitations as set forth above.

## **6. Retention Requirements**

Documents that are electronically filed and require original signatures other than that of the ECF User must be maintained in paper form by the ECF User until one year has passed after the time period for appeal expires. The ECF User must provide original documents for review upon request of the judge.

## **7. Signatures**

The user login and password required to submit documents to the ECF system serve as the ECF User's signature on all electronic documents filed with the court. They also serve as a signature for purposes under Rule 11(a) of the Federal Rules of Civil Procedure and any other purpose for which a signature is required in connection with proceedings before the court. Electronically filed documents must include a signature block and must set forth the name, address, telephone number and the attorney's state bar registration number, if applicable. In addition, the name of the ECF User under whose login and password the document is submitted must be preceded by an "s/" and typed in the space where the signature would otherwise appear.

Documents requiring multiple signatures, such as stipulations, shall be electronically filed as follows: (1) the ECF User shall obtain the signatures of all parties on the document; (2) the ECF User shall electronically file the document indicating the signatories in the format described above; and (3) a non-filing signatory or party who disputes the authenticity of an electronically filed document containing multiple signatures must file an objection to the document within ten days of receiving the Notice of Electronic Filing.

## **8. Service of Documents by Electronic Means**

When an ECF User electronically files a pleading or other documents using the ECF system, a Notice of Electronic Filing shall automatically be generated by the system, and shall be sent

automatically to all ECF registered parties entitled to service under Federal Rules of Civil Procedure and the Federal Rules of Criminal Procedure. Electronic service of the Notice of Electronic Filing constitutes service of the document to all such parties and shall be deemed to satisfy the requirement of Rule 5(b)(2)(D) of the Federal Rules of Civil Procedure and Rule 49(b) of the Federal Rules of Criminal Procedure.

All documents filed using the ECF system shall contain a Certificate of Service stating that the document has been filed electronically and is available for viewing and downloading from the ECF system. The Certificate of Service must identify the manner in which service on each party was accomplished, including any party who has not received electronic service.

Parties who have not received electronic service are entitled to receive a paper copy of any electronically filed pleading or other document. Service of such paper copy must be made according to the Federal Rules of Civil Procedure and the Federal Rules of Criminal Procedure.

In accordance with Rule 6(e) of the Federal Rules of Civil Procedure, service by electronic means is treated the same as service by mail.

## **9. Technical Failures**

A filing party whose filing is made untimely as the result of the technical failure of the court's ECF system may seek appropriate relief from the presiding judge.

## **10. Public Access**

The Office of the Clerk is now accepting electronically filed pleadings and making the content of these pleadings available on the court's Internet website via PACER. Any subscriber to PACER will be able to read, download, store and print the full content of electronically filed documents. The clerk's office will not make electronically available any documents that have been sealed or otherwise restricted by court order.

Any person or organization, other than one registered as an ECF User under Section 2 of this Procedural Order, may access ECF at the court's Internet site, [www.wied.uscourts.gov](http://www.wied.uscourts.gov), by obtaining a PACER login and password. Those who have PACER access, but who are not ECF Users, may retrieve docket sheets and those documents which the court makes available on the Internet for the fee normally charged for this service as set by the fee schedule authorized by the Administrative Office of the United States Courts, but they may not file documents.

With the exception of Social Security Appeals, documents in civil and criminal cases will be made available electronically to the same extent that they are available for personal inspection in the Office of the Clerk of Court at the U.S. Courthouse. Public remote access to documents in Social Security Appeals is limited to an opinion, order, judgment, or other disposition of the court. Complete access to these cases will be limited to attorneys of record.

In compliance with the E-Government Act of 2002, a party wishing to file a document containing the personal data identifiers specified below in an ECF case, may move to file an unredacted document under seal. This document shall be retained by the court as part of the record. The court may, however, still require the party to file a redacted copy for the public file.

Exercise caution when filing documents in an ECF case that contain the following:

- 1) Social Security numbers
- 2) financial account numbers
- 3) dates of birth
- 4) names of minor children
- 5) personal identifying numbers, such as a driver's license number
- 6) medical records, treatment and diagnosis
- 7) employment history
- 8) individual financial information
- 9) proprietary or trade secret information

Counsel is strongly urged to share this notice with all clients so that an informed decision about inclusion of certain materials may be made. **The clerk will not review each pleading for redaction.**

#### **11. Excluded Documents**

The following documents are presently excluded from the provisions of this Procedural Order. This list may be amended from time to time.

- 1) Civil Complaint
- 2) Criminal Indictment or Information
- 3) Criminal Plea Agreement
- 4) State Court Records
- 5) Social Security Transcripts
- 6) Documents exceeding five megabytes
- 7) All filings in criminal juvenile cases

**IT IS SO ORDERED,**

Dated at Milwaukee, Wisconsin, this 1<sup>st</sup> day of December, 2007.

s/ Rudolph T. Randa  
RUDOLPH T. RANDA  
Chief Judge

- (h) the approval of a disclosure statement;
- (i) the confirmation of a plan;
- (j) an objection to, or waiver or revocation of, the debtor's discharge;
- (k) any other matter in which the United States trustee requests copies of filed papers or the court orders copies transmitted to the United States trustee.

Notes

**Rule 9035. Applicability of Rules in Judicial Districts in Alabama and North Carolina**

In any case under the Code that is filed in or transferred to a district in the State of Alabama or the State of North Carolina and in which a United States trustee is not authorized to act, these rules apply to the extent that they are not inconsistent with any federal statute effective in the case.

Notes

**Rule 9036. Notice by electronic transmission**

Whenever the clerk or some other person as directed by the court is required to send notice by mail and the entity entitled to receive the notice requests in writing that, instead of notice by mail, all or part of the information required to be contained in the notice be sent by a specified type of electronic transmission, the court may direct the clerk or other person to send the information by such electronic transmission. Notice by electronic means is complete on transmission.

Notes

**Rule 9037. Privacy Protection For Filings Made with the Court**

**(a) Redacted filings.**

Unless the court orders otherwise, in an electronic or paper filing made with the court that contains an individual's social-security number, taxpayer-identification number, or birth date, the name of an individual, other than the debtor, known to be and identified as a minor, or a financial-account number, a party or nonparty making the filing may include only:

- (1) the last four digits of the social-security number and taxpayer-identification number;
- (2) the year of the individual's birth;
- (3) the minor's initials; and

**EXHIBIT**

**D**

(4) the last four digits of the financial-account number.

**(b) Exemptions from the redaction requirement.**

The redaction requirement does not apply to the following:

(1) a financial-account number that identifies the property allegedly subject to forfeiture in a forfeiture proceeding;

(2) the record of an administrative or agency proceeding unless filed with a proof of claim;

(3) the official record of a state-court proceeding;

(4) the record of a court or tribunal, if that record was not subject to the redaction requirement when originally filed;

(5) a filing covered by subdivision (c) of this rule; and

(6) a filing that is subject to § 110 of the Code.

**(c) Filings made under seal.**

The court may order that a filing be made under seal without redaction. The court may later unseal the filing or order the entity that made the filing to file a redacted version for the public record.

**(d) Protective orders.**

For cause, the court may by order in a case under the Code:

(1) require redaction of additional information; or

(2) limit or prohibit a nonparty's remote electronic access to a document filed with the court.

**(e) Option for additional unredacted filing under seal.**

An entity making a redacted filing may also file an unredacted copy under seal. The court must retain the unredacted copy as part of the record.

**(f) Option for filing a reference list.**

A filing that contains redacted information may be filed together with a reference list that identifies each item of redacted information and specifies an appropriate identifier that uniquely corresponds to each item listed. The list must be filed under seal and may be amended as of right. Any reference in the case to a listed identifier will be construed to refer to the corresponding item of

information.

(g) Waiver of protection of identifiers.

An entity waives the protection of subdivision (a) as to the entity's own information by filing it without redaction and not under seal.

Notes

**PART X—UNITED STATES TRUSTEES  
[ABROGATED]**

OFFICE OF THE GENERAL COUNSEL

MEMORANDUM GC 09-02

October 21, 2008

TO: All Division Heads, Regional Directors,  
Officers-in-Charge, and Resident Officers

FROM: Ronald Meisburg, General Counsel

SUBJECT: New Federal Rules Protecting Personal Identification  
Information in Court Filings

As you may already know, all federal rules of procedure now require that certain personal identification information be redacted from documents filed with the courts electronically or in paper form. See Rule 5.2 of the Federal Rules of Civil Procedure (FRCP); Rule 25(a)(5) of the Federal Rules of Appellate Procedure (FRAP); Rule 9037 of the Federal Rules of Bankruptcy Procedure (Bankr. Rule), Rule 49.1 of the Federal Rules of Criminal Procedure.<sup>1</sup> This memorandum underscores for all Agency employees the importance of complying with these rules when making court filings.

FRCP Rule 5.2, entitled "Privacy Protection for Filings Made with the Court," and all the other federal rules regulate paper court filings as well as electronic filings, and thus go further than required by the E-Government Act of 2002, which prompted these new requirements.<sup>2</sup>

**FRCP Rule 5.2:** The core provision of Rule 5.2 sets forth required redactions from court filings of personal data identifiers. These required redactions include Social Security and taxpayer-identification numbers, dates of birth, names of minor children, and financial-account numbers. Rule 5.2(a) provides:

(a) Redacted Filings. Unless the court orders otherwise, in an electronic or paper filing with the court that contains an individual's social-security number, taxpayer-identification

---

<sup>1</sup> The full text of FRCP 5.2, FRAP 25(a)(5), and Bankruptcy Rule 9037 are set forth in the attached Appendix.

<sup>2</sup> The Supreme Court has not issued a formal privacy redaction rule, but it has issued "Guidelines for Electronic Submission of Briefs on the Merits" that require the same redactions discussed herein for both paper and electronic submissions to the Court.

EXHIBIT

E

number, or birth date, the name of an individual known to be a minor, or a financial-account number, a party or nonparty making the filing may include only:

- (1) the last four digits of the social-security number and taxpayer-identification number;
- (2) the year of the individual's birth;
- (3) the minor's initials; and
- (4) the last four digits of the financial-account number.

Rule 5.2(b) sets forth limited exemptions from the redaction requirement. Most relevant to the NLRB is Rule 5.2(b)(2), which provides "[t]he redaction requirement does not apply to . . . the record of an administrative or agency proceeding." Accordingly, there is no requirement that the NLRB redact documents initially made part of the record of the underlying or collateral administrative proceeding and subsequently filed in federal court as an exhibit or as the Agency's record. This exemption does not apply, of course, to documents that the Agency initially creates for filing in a federal district court (e.g., 10(j) proceedings, subpoena enforcement proceedings). Such documents initially filed in district court must conform with the redaction requirements of Rule 5.2(a).

The Advisory Committee Notes to Rule 5.2 provide that the "responsibility to redact filings rests with counsel and the party or non-party making the filing." Thus, the clerk of a court is not required to review documents filed with the court for compliance with the rule. This underscores the NLRB's responsibility to protect the privacy of personal identification information contained in documents filed in the court. Indeed, filing information that should have been redacted under Rule 5.2 could expose the Agency to Privacy Act liability.

Many local court rules also address the protection of private information, and accordingly, should always be reviewed before filing in court. For example, the local rules for the United States District Court for the Western District of Missouri recommend that parties exercise caution when filing documents that contain private information beyond the items listed in Rule 5.2, such as driver's license numbers, medical records, and employment history.

**Federal Rules of Appellate, Bankruptcy, and Criminal Procedure:** As a practical matter, there is little difference between FRCP 5.2 and the rules applicable in the courts of appeals, the bankruptcy courts, or in criminal proceedings.

*FRAP 25(a) (5):* This rule provides for application of the privacy protection rule that applied to the case below to govern in the case on appeal, where the case below was governed by FRCP 5.2, Bankruptcy Rule 9037, or Criminal Rule 49.1. Where no such rule applied, as in Board proceedings pending enforcement under Sections 10(e) and (f) of the Act, privacy protection is governed by FRCP 5.2. Accordingly, in such cases, documents created for filing in the United States courts of appeals -- such as appellate court briefs and motions -- must conform with the redaction requirements of FRCP 5.2(a). Where a case in a United States court of appeals began in a district court, such as an appeal in a 10(j) case or subpoena enforcement case, FRCP 5.2 would also apply to all records created for filing in either court.

*Bankr. Rule 9037:* The redaction requirements of this rule are almost identical to FRCP 5.2. However, while Bankruptcy Rule 9037 contains the same exemption for "the record of an administrative or agency proceeding . . ." this exemption does *NOT apply to the record of an administrative or agency proceeding that is "filed with a proof of claim."* Bankr. Rule 9037(b) (2). Accordingly, when filing proofs of claim and attachments, the Regions must be careful to redact identifying information in accordance with Bankruptcy Rule 9037(a).

*Criminal Rule 49.1:* This rule is almost identical to FRCP 5.2, but includes the further requirement to redact an individual's home address to reveal only the city and state.

If court proceedings implicate compliance-related issues such as, for example, the possible institution of contempt proceedings, compliance-related investigative subpoenas, the Right to Financial Privacy Act, or the Federal Debt Collection Procedure Act, questions regarding these new privacy rules should be directed to the Contempt Litigation and Compliance Branch. Questions regarding other court proceedings should be directed to the Special Litigation Branch.

/s/  
R.M.

cc: NLRBU  
Release to the Public

Memorandum GC 09-02

## APPENDIX

### **FRCP Rule 5.2. Privacy Protection For Filings Made with the Court**

**(a) Redacted Filings.** Unless the court orders otherwise, in an electronic or paper filing with the court that contains an individual's social-security number, taxpayer-identification number, or birth date, the name of an individual known to be a minor, or a financial-account number, a party or nonparty making the filing may include only:

- (1) the last four digits of the social-security number and taxpayer-identification number;
- (2) the year of the individual's birth;
- (3) the minor's initials; and
- (4) the last four digits of the financial-account number.

**(b) Exemptions from the Redaction Requirement.** The redaction requirement does not apply to the following:

- (1) a financial-account number that identifies the property allegedly subject to forfeiture in a forfeiture proceeding;
- (2) the record of an administrative or agency proceeding;
- (3) the official record of a state-court proceeding;
- (4) the record of a court or tribunal, if that record was not subject to the redaction requirement when originally filed;
- (5) a filing covered by Rule 5.2(c) or (d); and
- (6) a pro se filing in an action brought under 28 U.S.C. §§ 2241, 2254, or 2255.

**(c) Limitations on Remote Access to Electronic Files; Social-Security Appeals and Immigration Cases.** Unless the court orders otherwise, in an action for benefits under the Social Security Act, and in an action or proceeding relating to an order of removal, to relief from removal, or to immigration benefits or detention, access to an electronic file is authorized as follows:

- (1) the parties and their attorneys may have remote electronic access to any part of the case file, including the administrative record;

(2) any other person may have electronic access to the full record at the courthouse, but may have remote electronic access only to:

- (A) the docket maintained by the court; and
- (B) an opinion, order, judgment, or other disposition of the court, but not any other part of the case file or the administrative record.

**(d) Filings Made Under Seal.** The court may order that a filing be made under seal without redaction. The court may later unseal the filing or order the person who made the filing to file a redacted version for the public record.

**(e) Protective Orders.** For good cause, the court may by order in a case: (1) require redaction of additional information; or (2) limit or prohibit a nonparty's remote electronic access to a document filed with the court.

**(f) Option for Additional Unredacted Filing Under Seal.** A person making a redacted filing may also file an unredacted copy under seal. The court must retain the unredacted copy as part of the record.

**(g) Option for Filing a Reference List.** A filing that contains redacted information may be filed together with a reference list that identifies each item of redacted information and specifies an appropriate identifier that uniquely corresponds to each item listed. The list must be filed under seal and may be amended as of right. Any reference in the case to a listed identifier will be construed to refer to the corresponding item of information.

**(h) Waiver of Protection of Identifiers.** A person waives the protection of Rule 5.2(a) as to the person's own information by filing it without redaction and not under seal.

---

**FRAP 25(a)(5): Privacy Protection.** An appeal in a case whose privacy protection was governed by Federal Rule of Bankruptcy Procedure 9037, Federal Rule of Civil Procedure 5.2, or Federal Rule of Criminal Procedure 49.1 is governed by the same rule on appeal. In all other proceedings, privacy protection is governed by Federal Rule of Civil Procedure 5.2, except that Federal Rule of Criminal Procedure 49.1 governs when an extraordinary writ is sought in a criminal case."

---

**Bankruptcy Rule 9037: Privacy Protection For Filings Made with the Court.**

**(a) Redacted Filings.** Unless the court orders otherwise, in an electronic or paper filing made with the court that contains an individual's social-security number, taxpayer-identification number, or birth date, the name of an individual, other than the debtor, known to be and identified as a minor, or a financial-account number, a party or nonparty making the filing may include only:

- (1) the last four digits of the social-security number and taxpayer-identification number;
- (2) the year of the individual's birth;
- (3) the minor's initials; and
- (4) the last four digits of the financial-account number.

**(b) Exemptions From the Redaction Requirement.** The redaction requirement does not apply to the following:

- (1) a financial-account number that identifies the property allegedly subject to forfeiture in a forfeiture proceeding;
- (2) the record of an administrative or agency proceeding unless filed with a proof of claim;
- (3) the official record of a state-court proceeding;
- (4) the record of a court or tribunal, if that record was not subject to the redaction requirement when originally filed;
- (5) a filing covered by subdivision (c) of this rule; and
- (6) a filing that is subject to § 110 of the Code.

**(c) Filings Made Under Seal.** The court may order that a filing be made under seal without redaction. The court may later unseal the filing or order the entity that made the filing to file a redacted version for the public record.

**(d) Protective Orders.** For cause, the court may by order in a case under the Code:

- (1) require redaction of additional information; or
- (2) limit or prohibit a nonparty's remote electronic access to a document filed with the court.

**(e) Option For Additional Unredacted Filing Under Seal.** An entity making a redacted filing may also file an unredacted copy under seal. The court must retain the unredacted copy as part of the record.

**(f) Option For Filing A Reference List.** A filing that contains redacted information may be filed together with a reference list that identifies each item of redacted information and specifies

an appropriate identifier that uniquely corresponds to each item listed. The list must be filed under seal and may be amended as of right. Any reference in the case to a listed identifier will be construed to refer to the corresponding item of information.

**(g) Waiver of Protection of Identifiers.**

An entity waives the protection of subdivision (a) as to the entity's own information by filing it without redaction and not under seal.



FOLEY & LARDNER LLP

ATTORNEYS AT LAW

777 EAST WISCONSIN AVENUE  
MILWAUKEE, WI 53202-5306  
414.271.2400 TEL  
414.297.4900 FAX  
foley.com

WRITER'S DIRECT LINE  
414.297.5773  
fdicastro@foley.com EMAIL

CLIENT/MATTER NUMBER  
010124-0609

January 9, 2009

**VIA ELECTRONIC DELIVERY**

Honorable James E. Shapiro  
U.S. Bankruptcy Court  
517 East Wisconsin Avenue  
Milwaukee, WI 53202

Re: In Re Daniel E. Ottow and Mirjana Otto  
Case No. 07-28378-jes

Daniel Evans Ottow v. Aurora Health Care  
Adversary Proc. No. 08-02274

Dear Judge Shapiro:

I write to advise the Court that Mr. and Mrs. Ottow and Aurora Health Care have reached an agreement in principle to settle the adversary complaint against Aurora in the above matter. Accordingly, the parties jointly request that the briefing schedule on Aurora's motion to dismiss be stayed until a written settlement agreement can be finalized, at which time the parties will submit a stipulation and order for dismissal with prejudice, on the merits, and without an award of fees or costs to any party. Accordingly, Aurora also requests the Court to excuse it from the pre-trial conference that is set for January 15, 2009. Thank you for Your Honor's consideration of these requests.

Very truly yours,

s/ Frank W. DiCastri

Frank W. DiCastri

cc: Michael P. Maxwell, Esq.

BOSTON  
BRUSSELS  
CENTURY CITY  
CHICAGO  
DETROIT

JACKSONVILLE  
LOS ANGELES  
MADISON  
MIAMI  
MILWAUKEE

NEW YORK  
ORLANDO  
SACRAMENTO  
SAN DIEGO  
SAN DIEGO/DEL MAR

SAN FRANCISCO  
SHANGHAI  
SILICON VALLEY  
TALLAHASSEE  
TAMPA

TOKYO  
WASHINGTON, D.C.

EXHIBIT

F

UNITED STATES BANKRUPTCY COURT  
EASTERN DISTRICT OF WISCONSIN

In re: )  
OTTOW, DANIEL EVANS ) Chapter 7  
OTTOW, MIRJANA )  
Debtors. ) Case No. 07-28378 JES  
OTTOW, DANIEL EVANS )  
Plaintiff, ) Adversary Proceeding No. 08-02274  
vs. )  
AURORA HEALTH CARE, INC. )  
Defendant. )

**STIPULATION FOR DISMISSAL**

The parties, by their undersigned attorneys, hereby stipulate and agree that this action may be dismissed on its merits, with prejudice, and without an award of fees or costs to any party.

Dated this 30<sup>th</sup> day of March, 2009.

MICHAEL P. MAXWELL



One of the Attorneys for Plaintiff Daniel Evans  
Ottow

Prepared by:

Frank W. DiCastri  
FOLEY & LARDNER LLP  
777 East Wisconsin Avenue  
Milwaukee, Wisconsin 53202  
(414) 271-2400  
(414) 297-4900  
fdicastri@foley.com

MILW\_8484541.1

MAXWELL ATTORNEYS LLC  
8112 W. Bluemound Road, Suite 61  
Wauwatosa, WI 53213  
(414) 727-0123  
(414) 727-0124 (fax)

Dated this 2<sup>nd</sup> day of April, 2009.

FRANK W. DICASTRI



---

One of the Attorneys for Defendant Aurora  
Health Care, Inc.

FOLEY & LARDNER LLP  
777 East Wisconsin Avenue  
Milwaukee, WI 53202-5367  
(414) 271-2400 (Main)  
(414) 297-5826 (BFR)  
(414) 297-4900 (fax)